Management Software

AT-S79

User's Guide

For use with the AT-GS950/16 and AT-GS950/24 Gigabit Ethernet Smart Switches

Version 1.1

613-000207 Rev. B

Allied Telesyn

Contents

Figures

Tables

Preface

This guide contains instructions on how to use the AT-S79 management software to manage and monitor the AT-GS950/16 and AT-GS950/24 Gigabit Ethernet Smart switches.

The AT-S79 management software has two management interfaces: a menus interface and a web browser interface. You access the menus interface through the console port on the switch. You access the web browser interface from any management workstation on your network that has a web browser application. For background information on the management interfaces, refer to Chapter 1, “Overview” on page 15.

Note
The AT-S79 management software does not support remote management with the Telnet application protocol or an SNMP program.

Note
The interface illustrations in this book show the interface for the AT-GS960/16 Gigabit Ethernet Smart Switch. With the exception of the number of ports displayed, the features also apply to the AT-GS9500/24 Gigabit Ethernet Smart Switch.

This preface contains the following sections:

Where to Find Web-based Guides

The installation and user guides for all Allied Telesyn products are available in portable document format (PDF) on our web site at **www.alliedtelesyn.com**. You can view the documents online or download them onto a local workstation or server.

Document Conventions

This document uses the following conventions:

Note
Notes provide additional information.

Caution
Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

Warning
Warnings inform you that performing or omitting a specific action may result in bodily injury.

Contacting Allied Telesyn

This section provides Allied Telesyn contact information for technical support as well as sales and corporate information.

Online Support

You can request technical support online by accessing the Allied Telesyn Knowledge Base: **http://kb.alliedtelesyn.com**. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

Email and Telephone Support

For Technical Support via email or telephone, refer to the Support & Services section of the Allied Telesyn web site: **www.alliedtelesyn.com**.

Returning Products

Products for return or repair must first be assigned a return materials authorization (RMA) number. A product sent to Allied Telesyn without an RMA number will be returned to the sender at the sender's expense.

To obtain an RMA number, contact Allied Telesyn Technical Support through our web site: **www.alliedtelesyn.com**.

Sales or Corporate Information

You can contact Allied Telesyn for sales or corporate information through our web site: **www.alliedtelesyn.com**. To find the contact information for your country, select Contact Us -> Worldwide Contacts.

Management Software Updates

New releases of management software for our managed products are available from either of the following Internet sites:

- Allied Telesyn web site: **www.alliedtelesyn.com**
- Allied Telesyn FTP server: **ftp://ftp.alliedtelesyn.com**

To download new software from the Allied Telesyn FTP server from your workstation's command prompt, you must have FTP client software. Additionally, you must log in to the server. The user name is "anonymous" and your email address is the password.

Chapter 1
Overview

This chapter provides an overview of the AT-S79 management software for the AT-GS950/16 and AT-GS950/24 switches. The chapter describes the different methods for accessing the software and the management access levels. This chapter contains the following sections:

Management Overview

The AT-S79 management software allows you to view and adjust the operating parameters of the AT-GS950/16 and AT-GS950/24 Smart Switches. Here are a few examples of the functions that you can perform with the management software:

- Enable and disable ports
- Configure a port's speed and duplex mode
- Create port trunks
- Configure a port mirror
- Configure Quality of Service (QoS)
- Create port-based and tagged virtual LANs
- Configure 802.1x port-based network access control

The AT-S79 management software comes preinstalled on the switch with default settings for all of the switch's operating parameters. You do not have to manage the switch if the default settings are adequate for your network. Instead, you can use the device as an unmanaged switch by connecting it to your network, as explained in the hardware installation guide, and powering on the unit.

Note
The default settings for the management software are listed in Appendix A, "AT-S79 Software Default Settings" on page 237.

To actively manage the switch and adjust its operating parameters, you must access the switch's AT-S79 management software. There are two ways to manage the switch:

- Local management using the menus interface
- Remote management using the web browser interface

The chapters in Section I of this guide explain how to manage the switch from a local management session using the menu interface, while the chapters in Section II explain how to manage the device from a remote session using the web browser interface. Both interfaces allow you to configure all parameters on the switch.

The following sections in this chapter briefly describe each type of management connection.

Local Management Connection

To establish a local management connection with an AT-GS950/16 or AT-GS950/24 Smart Switch, you connect a terminal or a PC with a terminal emulator program to the terminal port on the front of the switch using the management cable included with the unit. This type of connection is referred to as "local" because you must be physically close to the switch, such as in the wiring closet where the switch is located.

Note
For instructions on how to start a local management session, refer to "Starting a Local Management Session" on page 24.

A switch does not need an Internet Protocol (IP) address for you to manage it locally. You can start a local management session on a switch at any time. It does not interfere with the forwarding of network packets by the device.

Remote Management Connection

The AT-S79 management software has a web browser interface that you can use to manage an AT-GS950/16 or AT-GS950/24 Smart Switch from any management station on your network that has a web browser application. This is referred to as a remote connection.

The switch must have an IP address in order for you to manage it remotely with a web browser. You can assign the switch an IP address manually or you can activate the DHCP client so that the switch automatically obtains its IP configuration from a DHCP server on the network. The initial assignment of an IP address on a switch must be made through a local connection to the unit.

For instructions on how to start a remote management session, refer to “Establishing a Remote Connection to Use the Web Browser Interface” on page 158.

Note
In order to remotely manage a switch using a web browser, the remote management station must be a member of the switch’s Default VLAN. The switch processes remote management packets only when they are received on an untagged port of the Default VLAN.

Note
The AT-S79 management software does not support remote management with the Telnet application protocol or an SNMP application program.

Management Access Level

The AT-S79 management software has one level of management access: manager. When you log in as a manager, you can view and configure all of a switch's operating parameters. You log in as a manager by entering the appropriate username and password when you start an AT-S79 management session. The default username and password are both "manager".

Ports 15 and 16 on the AT-GS950/16 Switch and Ports 23 and 24 on the AT-GS950/24 Switch

This section applies to the twisted pair and optional SFP ports 15 and 16 on the AT-GS950/16 switch and ports 23 and 24 on the AT-GS950/24 switch. Note the following when configuring these ports:

- The twisted pair ports are, by default, the active ports.
- An optional SFP port becomes active when it establishes a link with an end node, at which point the corresponding twisted pair port changes to the redundant state.
- A twisted pair port and its corresponding optional SFP port share the same configuration settings, including port settings and VLAN assignments. When an SFP port establishes a link with an end node, it operates with the same settings as its corresponding twisted pair port.

Section I

Using the Menus Interface

The chapters in this section explain how to manage the switch using the menus interface of the AT-S79 management software. The chapters include:

Chapter 2

Getting Started with the Menus Interface

This chapter provides information and instructions on how to access the menus interface of the AT-S79 management software by starting a local management session. This chapter contains the following sections:

Starting a Local Management Session

You establish a local management session with the switch by connecting a terminal or personal computer with a terminal emulation program to the the RS-232 console port on the front panel of the switch.

Note
You do not need to assign an IP address to the switch to manage the unit from a local management session.

To start a local management session, perform the following procedure:

1. Connect one end of the management cable included with the switch to the console port on the switch, as shown in Figure 1.

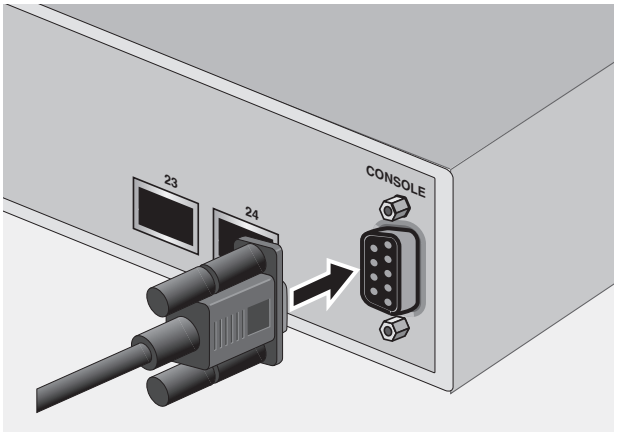


Figure 1. Connecting the Management Cable to the Console Port

2. Connect the other end of the cable to the RS-232 port on a terminal or PC with a terminal emulator program.
3. Configure the terminal or terminal emulator program as follows:
   - ❒ Baud per second: 9600
   - ❒ Data bits: 8
   - ❒ Stop bits: 1
   - ❒ Flow control: None

Note
These settings are for a DEC VT100 or ANSI terminal, or an equivalent terminal emulation program. They cannot be changed.

The Login Menu is shown in Figure 2.

```
AT-GS950/16 Local Management System
Enter the character in square brackets to select option

Login Menu

Login:
```

Figure 2. Login Menu

4. Enter the manager login name and press Return. The default name is "manager".

   You are prompted for a password.

5. Enter the manager password. The default password is "manager".

> **Note**
> To change the login name or password, refer to "Setting the User Interface Configuration" on page 36.

The Main Menu is shown in Figure 3.

```
AT-GS950/16 Local Management System
Enter the character in square brackets to select option

Main Menu

[G]eneral Information
[B]asic Switch Configuration
[A]dvanced Switch Configuration
Switch [T]ools
[S]tatistics
[Q]uit




Command>
```

Figure 3. Main Menu

Using the Menus Interface

If you are using a DEC VT00 or ANSI (the default) terminal configuration, refer to Table 1 for instructions on how to move through the menus and select menu options.

Table 1. Menus Interface Operations

When directed to	You must
Enter your selection	Type the menu option letter.
Enter information (for example, entering a port number)	Type the information and press Enter.
Return to previous menu	Type Q for Quit to Previous Menu.

When you press Enter to select a field in which you can enter a value, the “>” symbol is displayed. For example:

```
Enter new password>
```

The “>” symbol indicates that you can enter a new value for the parameter or change the existing value. After you have entered a value, press Enter. Changes are immediately activated on the AT-GS950 Series switch.

Quitting from a Local Management Session

To quit a local management session, return to the Main Menu and type **Q** for Quit. When you are finished managing the switch, make sure you exit from a management session. Quitting from a local session prevents unauthorized changes to the switch's configuration if you leave your workstation unattended.

Note
A local management session automatically times out if there is no management activity during a pre-defined length of time referred to as the timeout period. The timeout feature is intended to protect the parameter settings on the switch from unauthorized changes should you leave your management station unattended during a management session. The default timeout value is 10 minutes. To change the timeout default value, refer to "Setting the User Interface Configuration" on page 36.

Chapter 3

Basic Switch Parameters

This chapter contains the following sections:

Configuring the IP Address, Subnet Mask, and Gateway Address

This procedure explains how to manually assign an IP address, subnet mask, and gateway address to the switch. Before performing the procedure, note the following:

- An IP address and subnet mask are not required for normal network operations of the switch. Values for these parameters are only required if you want to remotely manage the device with a web browser.
- A gateway address is only required if you want to remotely manage the device from a remote management station that is separated from the switch by a router.
- To configure the switch to automatically obtain its IP configuration from a DHCP server on your network, go to “Enabling and Disabling the DHCP Client” on page 33.

To set the switch’s IP configuration, perform the following procedure:

1. From the Main Menu, type **B** to select **Basic Switch Configuration**.

   The Basic Switch Configuration Menu is shown in Figure 4.

```
AT-GS950/16 Local Management System
Main Menu -> Basic Switch Configuration Menu

System [A]dministration Configuration
System [I]P Configuration
[P]ort Configuration
[U]ser Interface Configuration
Storm [C]ontrol Configuration
[Q]uit to previous menu









Command>
```

Figure 4. Basic Switch Configuration Menu

2. From the Basic Switch Configuration Menu, type **I** to select **System IP Configuration**.

   The System IP Configuration Menu is shown in Figure 5.

```
AT-GS950/16 Local Management System
Basic Switch Configuration -> System IP Configuration Menu

MAC Address:    00:06:5H:B2:65:84
IP Address:     0.0.0.0
Subnet Mask:    0.0.0.0
Gateway:        0.0.0.0
DHCP Mode:      Disabled


----------------------- <COMMAND> -----------------------------
Set [I]P Address
Set Subnet [M]ask
Set Default [G]ateway
Enable/Disable [D]HCP Mode
[Q]uit to previous menu


Command>
```

Figure 5. System IP Configuration Menu

The top portion of the menu displays the current IP address, subnet mask, and gateway address for the switch. The menu also displays the switch's MAC address. The MAC address cannot be changed. The menu also displays the current status of the DHCP client on the switch.

The Enable/Disable DHCP Mode option is described in "Enabling and Disabling the DHCP Client" on page 33.

3. To set the switch's IP address, do the following:

   a. Type **I** to select **Set IP Address**.

      The following prompt is displayed:

      ```
      Enter new IP address>
      ```

   b. Type the IP address for the switch and press Enter.

4. To set the switch's subnet mask, do the following:

   a. Type **M** to select **Set Subnet Mask**.

      The following prompt is displayed:

      ```
      Enter new subnet mask>
      ```

b. Type the subnet mask for the switch and press Enter.

5. To set the switch's gateway address, do the following:

   a. Type **G** to select **Set Default Gateway**.

      The following prompt is displayed:

      ```
      Enter new gateway IP address>
      ```

   b. Type the gateway IP address for the switch and press Enter.

6. Type **Q** to select **Quit to previous menu** and save your changes.

Enabling and Disabling the DHCP Client

This procedure explains how to activate and deactivate the DHCP client on the switch. When the client is activated, the switch obtains its IP configuration, such as its IP address and subnet mask, from a DHCP server on your network. Before performing the procedure, note the following:

- An IP address and subnet mask are not required for normal network operations of the switch. Values for these parameters are only required if you want to remotely manage the device with a web browser.
- A gateway address is only required if you want to remotely manage the device from a remote management station that is separated from the switch by a router.
- The DHCP client is disabled by default on the switch.
- The DHCP client does not support BOOTP servers.

To activate or deactivate the DHCP client on the switch, perform the following procedure:

1. From the Main Menu, type **B** to select **Basic Switch Configuration**.

   The Basic Switch Configuration Menu is shown in Figure 4 on page 30.

2. From the Basic Switch Configuration Menu, type **I** to select **System IP Configuration**.

   The System IP Configuration Menu is shown in Figure 5 on page 31.

3. Type **D** to select **Enable/Disable DHCP Mode**.

   The following prompt is displayed:

   ```
   Enable or Disable DHCP mode (E/D)>
   ```

4. Type **E** to select Enable or **D** to select Disable.

   If you enable the client, it immediately begins to send queries to the DHCP server. It continues to send queries until it receives a response.

5. Type **Q** to select **Quit to previous menu** and save your changes.

Configuring System Administration Information

This section explains how to assign a name to the switch, as well as specify the location of the switch and the name of the switch's administrator. Entering this information is optional.

To set a switch's administration information, perform the following procedure:

1. From the Main Menu, type **B** to select **Basic Switch Configuration**.

   The Basic Switch Configuration Menu is shown in Figure 4 on page 30.

2. From the Basic Switch Configuration Menu, type **A** to select **System Administration Information**.

   The System Administration Configuration Menu is shown in Figure 6.

```
AT-GS950/16 Local Management System
Basic Switch Configuration -> System Admin. Configuration Menu

Description:   AT-GS950/16
Name:
Location:
Contact:



---------------------- <COMMAND> -----------------------------
Set System [N]ame
Set System [L]ocation
Set System [C]ontact Information
[Q]uit to previous menu


Command>
```

Figure 6. System Administration Configuration Menu

   The Description parameter in the top portion of the menu displays the model name of the switch. This parameter cannot be changed.

3. To set the system's name, do the following:

   a. Type **N** to select **Set System Name**.

      The following prompt is displayed:

      ```
      Enter system name>
      ```

b. Type a name for the switch (for example, Sales). The name is optional and can contain up to 50 characters.

Note
Allied Telesyn recommends that you assign names to the switches. Names can help you identify the switches when you manage them and can also help you avoid performing a configuration procedure on the wrong switch.

4. To enter the system's location, do the following:

   a. Type **L** to select **Set System Location**.

      The following prompt is displayed:

      ```
      Enter system location>
      ```

   b. Type information to describe the location of the switch (for instance, Third Floor). The location is optional and can contain up to 50 characters.

5. To enter the administrator's name, do the following:

   a. Type **C** to select **Set System Contact Information**.

      The following prompt is displayed:

      ```
      Enter system contact>
      ```

   b. Type the name of the network administrator responsible for managing the switch. The contact name is optional and can contain up to 50 characters.

6. Type **Q** to select **Quit to previous menu** and save your changes.

Setting the User Interface Configuration

This procedure explains how to adjust the user interface and security features on the switch. With this procedure you can:

- Change the console timer, used to automatically end inactive local management sessions.
- Change the AT-S79 management login user name and password.
- Enable and disable the web server, used to manage the switch from a remote management station with a web browser.

To set the switch's user interface configuration, perform the following procedure:

1. From the Main Menu, type **B** to select **Basic Switch Configuration**.

   The Basic Switch Configuration Menu is shown in Figure 4 on page 30.

2. From the Basic Switch Configuration Menu, type **U** to select **User Interface Configuration**.

   The User Interface Configuration Menu is shown in Figure 7.

```
AT-GS950/16 Local Management System
Basic Switch Configuration -> User Interface Configuration Menu

Console UI Idle Timeout:  5 Min.

Web Server:    Enabled
User Name:     manager


---------------------- <COMMAND> -----------------------------
Set [C]onsole UI Time Out          Enable/Disable [W]eb Server
Change Administrator User [N]ame   [R]ADIUS Server Configuration
Change Administrator [P]assword    [Q]uit to previous menu


Command>
```

Figure 7. User Interface Configuration Menu

The RADIUS Server Configuration option is described Chapter 11, "RADIUS Authentication Protocol" on page 141.

3. To configure the console idle time out parameter, do the following:

   a. Type **C** to select **Set Console UI Time Out.**

      The following prompt is displayed:

      ```
      Enter console idle timeout>
      ```

   b. Enter a number for the timeout value. The range is 0 to 60 minutes. The default is 5 minutes. A timeout value to 0 causes the switch to never timeout a local management session.

      The console idle time out parameter specifies the length of time a local management session can be inactive before the management software automatically ends it. The purpose of this parameter is to prevent unauthorized individuals from configuring the switch should you leave your management workstation unattended.

      This parameter applies to a local management session but not to a remote web management session. A web browser management session remains active so long as your web browser is open.

      Note
      If you select 0, you must always remember to properly log off from a local management session when you are finished to prevent blocking future management sessions with the switch.

4. To enable or disable the web server, do the following:

   a. Type **W** to select **Enable/Disable Web Server**.

      The following prompt is displayed:

      ```
      Enable or Disable web server (E/D)>
      ```

   b. Type **E** to enable the web server or **D** to disable it. The default is enabled. If you disable the web server, you can not manage the switch from a remote management station using a web browser.

5. To change the AT-S79 management login user name, do the following:

   a. Type **N** to select **Change Administrator User Name**.

      The following prompt is displayed:

      ```
      Enter current password>
      ```

   b. Enter the current login password. The management software prompts you for the password to prevent an unauthorized individual from changing the login name.

c. Type the new user name and press Enter. The default name is “manager.” The name can be from 0 to 12 characters. Spaces are allowed. The login name is case sensitive. Not entering a new login name deletes the current login name without assigning a new one.

   The new user name appears in the User Field in the top portion of the menu. You must use the new login user name the next time you start a local or web browser management session.

6. To change the manager login password, do the following:

   a. Type **P** to select **Change Administrator Password**.

      The following prompt is displayed:

      ```
      Enter old password>
      ```

   b. Enter the current manager password and press Enter.

      The following prompt is displayed:

      ```
      Enter new password>
      ```

   c. Type the new password and press Enter. The password can be from 0 to 12 characters. Allied Telesyn recommends not using special characters, such as spaces and exclamation points. The password is case sensitive. Not entering a new password deletes the current password without assigning a new one.

      The following prompt is displayed:

      ```
      Retype new password>
      ```

   d. Retype the new password and press Enter.

      You must use the new login password the next time you start a local or web browser management session.

7. Type **Q** to select **Quit to previous menu** and save your changes.

Viewing Switch Information

To view general information about the switch, perform the following procedure:

1. From the Main Menu, type **G** to select **General Information**.

   The General Information menu is shown in Figure 8.

```
AT-GS950/16 Local Management System
Main Menu -> General Information

System up for : 24min(s), 36sec(s)

Runtime Image : Version 1.0
Boot Loader    : Version 1.0
Hardware Information
  Version:                          DRAM Size:    16MB
  Fixed Baud Rate:   9600bps        Flash Size:   4 MB
Administration Information
  Switch Name: Marketing
  Switch Location: Fourth Floor
  Switch Contact: Ralph
System Address Information
  MAC Address:       00:06:5H:B2:65:84
  IP Address:        149.35.8.237
  Subnet Mask:       255.255.255.0
  Gateway:           149.35.8.1
Automatic Network Features
  DHCP Mode:         Disabled



Press any key to continue...
```

Figure 8. General Information Menu

The General Information Menu displays the following information:

System up for
The number of hours, minutes, and seconds since the last reset or power cycle.

Runtime Image
The version of the runtime software.

Boot Loader
The version of the boot loader software.

Hardware Information Section

Version
The hardware version number.

Fixed Baud Rate
The baud rate of the console port.

DRAM Size
The size of the DRAM, in megabytes.

Flash Size
The size of the flash memory, in megabytes.

Administration Information Section

Switch Name
The name assigned to the switch. To assign the switch a name, refer to “Configuring System Administration Information” on page 34.

Switch Location
The location of the switch. To specify the location, refer to “Configuring System Administration Information” on page 34.

Switch Contact
The contact person responsible for managing the switch. To specify the name of a contact, refer to “Configuring System Administration Information” on page 34.

System Address Information Section

MAC Address
The MAC address of the switch. You cannot change this information.

System IP Address
The IP address of the switch. Refer to “Configuring the IP Address, Subnet Mask, and Gateway Address” on page 30 to manually assign an IP address or “Enabling and Disabling the DHCP Client” on page 33 to activate the DHCP client.

Subnet Mask
The subnet mask for the switch. Refer to “Configuring the IP Address, Subnet Mask, and Gateway Address” on page 30 to manually assign a subnet mask or “Enabling and Disabling the DHCP Client” on page 33 to activate the DHCP client.

Gateway
Default gateway IP address. Refer to “Configuring the IP Address, Subnet Mask, and Gateway Address” on page 30 to manually assign a gateway address or “Enabling and Disabling the DHCP Client” on page 33 to activate the DHCP client.

Automatic Network Features Section

DHCP Mode
The status of the DHCP client on the switch. For information about setting this parameter, refer to "Enabling and Disabling the DHCP Client" on page 33.

2. Press any key to return to the previous menu.

Rebooting the Switch

This procedure reboots the switch and reloads the AT-S79 management software from flash memory. You might reboot the device if you believe it is experiencing a problem. Rebooting the device does not change any of the device's parameter settings.

Caution
The switch does not forward network traffic during the reboot process. Some network traffic may be lost.

To reboot the switch, perform the following procedure:

1. From the Main Menu type **T** to select **Switch Tools**.

   The Switch Tools Configuration Menu is shown in Figure 9.

```
AT-GS950/16 Local Management System
Main Menu -> Switch Tools Configuration Menu

Software [U]pgrade...
System [R]eboot
[P]ing Execution
[Q]uit to previous menu




Command>
```

Figure 9. Switch Tools Configuration Menu

2. From the Switch Tools Configuration Menu, type **R** to select **System Reboot**.

The System Reboot Menu is shown in Figure 10.

```
AT-GS950/24 Local Management System
Main Menu -> System Reboot Menu

Reboot Status:        Stop
Reboot Type:          Normal

---------------------- <COMMAND> ----------------------------

Set Reboot [O]ption
Start [R]eboot Process
[Q]uit to previous menu




Command>
```

Figure 10. System Reboot Menu

3. From the System Reboot menu, type **O** to select **Set Reboot Option**.

   The following prompt is displayed:

   ```
   Select reboot option (F/I/N)>
   ```

4. Type **N** to select **Normal**.

   Note
   The **F** and **I** options are described in "Returning the AT-S79 Management Software to the Factory Default Values" on page 47.

5. Type **R** to select **Start Reboot Process**.

   The following prompt is displayed:

   ```
   Are you sure you want to reboot the system (Y/N)>
   ```

6. Type **Y** to start the reboot process or **N** to cancel the reboot.

   The switch immediately begins to reload the AT-S79 management software. This process takes approximately one minute to complete. You can not manage the device during the reboot. After the reboot is finished, you can log in again if you want to continue to manage the device.

Pinging a Remote System

This procedure instructs the switch to ping a node on your network. This procedure is useful in determining whether an active link exists between the switch and another network device. Note the following before performing the procedure:

- The switch where you are initiating the ping must have an IP address and subnet mask.
- The device you are pinging must be a member of the Default VLAN. This means that the port on the switch through which the node is communicating with the switch must be an untagged or tagged member of the Default VLAN.

To ping a network device, perform the following procedure:

1. From the Main Menu, type **T** to select **Switch Tools**.

   The Switch Tools Configuration Menu is shown in Figure 9 on page 42.

2. From the Switch Tools Configuration Menu, type **P** to select **Ping Execution**.

   The Ping Execution Menu is shown in Figure 11.

```
AT-GS950/16 Local Management System
Switch Tools Configuration -> Ping Execution

Target IP Address:    0.0.0.0
Number of Requests:   10
Timeout Value (sec):  3
================Result================




---------------------- <COMMAND> -----------------------------
Set Target [I]P Address             [E]xecute Ping
Set [N]umber of Requests            [S]top Ping
Set [T]imeout Value                 [Q]uit to previous menu


Command>
```

Figure 11. Ping Execution Menu

3. Type **I** to select **Set Target IP Address**.

   The following prompt is displayed:

   ```
   Enter new target IP address>
   ```

4. Type the IP address of the node you want the switch to ping and press Enter.

5. Type **N** to select **Set Number of Requests**.

   The following prompt is displayed:

   ```
   Enter new number of requests>
   ```

6. Enter the number of ping requests you want the switch to perform. The range is 1 to 10. The default is 10.

7. Type **T** to select **Set Timeout Value**.

   The following prompt is displayed:

   ```
   Enter new timeout value>
   ```

8. Enter the length of time in seconds the switch is to wait for a response before assuming that a ping has failed. The range is 1 to 5 seconds. The default is 3 seconds.

9. Type **E** to select **Execute Ping**.

   The following prompt is displayed:

   ```
   Execute ping or Clean ping data (E/C)>
   ```

10. Type **E** to execute the ping or **C** to clear previous ping data before performing this ping.

Figure 12 shows an example of the results of a ping.

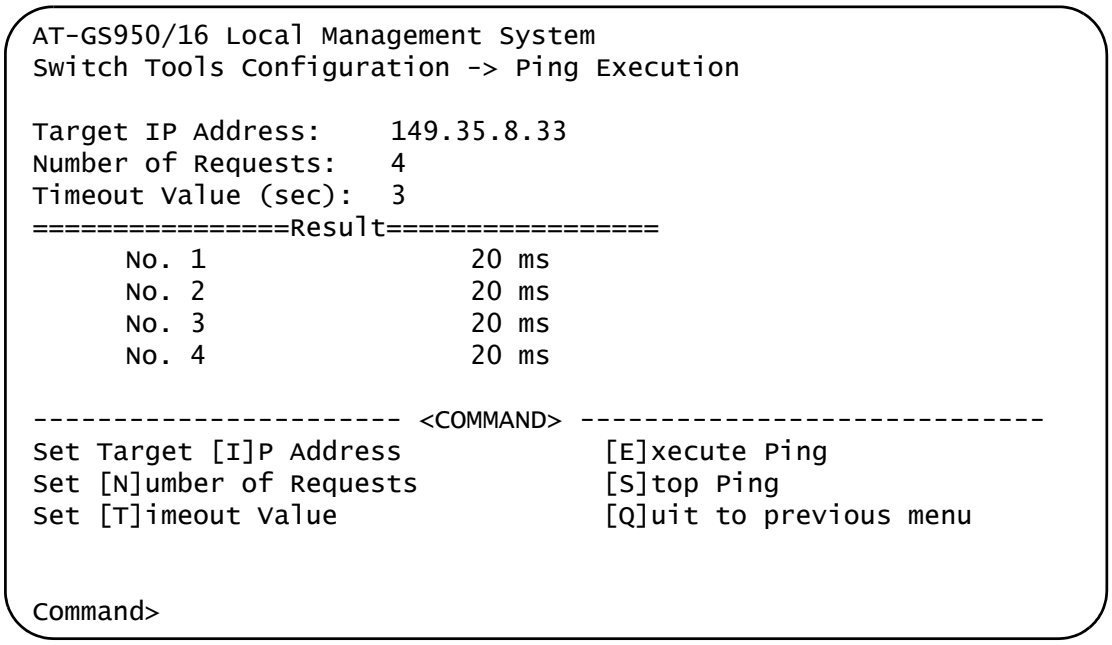


Figure 12. Ping Results

11. To stop the ping, type **S** to select **Stop Ping**.
12. Type **Q** to select **Quit to previous menu**.

Returning the AT-S79 Management Software to the Factory Default Values

This procedure returns all AT-S79 management software parameters to their default values and deletes all tagged and port-based VLANs on the switch. The AT-S79 management software default values are listed in Appendix A, "AT-S79 Software Default Settings" on page 237.

Caution
This procedure causes the switch to reboot. The switch does not forward network traffic during the reboot process. Some network traffic may be lost.

To return the AT-S79 management software to the default settings, perform the following procedure:

1. From the Main Menu, type **T** to select **Switch Tools**.

   The Switch Tools Configuration Menu is shown in Figure 9 on page 42.

2. From the Switch Tools Menu, type **R** to select **System Reboot** to start the reboot.

   The System Reboot menu is shown in Figure 10 on page 43.

3. Type **O** to select **Set Reboot Option**.

   The following prompt is displayed:

   ```
   Select reboot option (F/I/N)>
   ```

4. Type **F** or **I** to select one of the following:

   F (Factory Default)
   Resets all switch parameters to the factory default settings, including IP address, subnet mask, and gateway address.

   I (Reset to Defaults Except IP Address)
   Resets all switch parameters to the factory default settings, but retains the IP address, subnet mask, and gateway settings. If the DHCP client is enabled, it remains enabled after this reset.

   Note
   Option **N** is described in "Rebooting the Switch" on page 42.

5. Type **R** to select **Start Reboot Process**.

   The following prompt is displayed:

   ```
   Are you sure you want to reboot the system (Y/N)>
   ```

6. Type **Y** to start the reboot process.

   The switch returns its operating parameters to the default values and begins to reload the AT-S79 management software. This process takes approximately one minute to complete. You can not manage the device during the reboot. After the reboot is finished, you can log in again if you want to continue to manage the device.

Chapter 4

Port Configuration

This chapter contains the procedures for viewing and adjusting the parameter settings for the ports on the switch. This chapter contains the following sections:

Displaying the Port Parameters

To display the parameter settings for the ports on the switch, perform the following procedure:

1. From the Main Menu, type **B** to select **Basic Switch Configuration**.

   The Basic Switch Configuration Menu is shown in Figure 4 on page 30.

2. From the Basic Switch Configuration Menu, type **P** to select **Port Configuration**.

   The Port Configuration Menu is shown in Figure 13.

```
AT-GS950/16 Local Management System
Basic Switch Configuration -> Port Configuration Menu

Port  Trunk      Type     Link   Status     Mode            Flow Ctrl
----  -----      ------   ----   ------     --------------------
 1    ---        1000tx   Up     Enabled    Auto  (100F)    Enabled
 2    ---        1000tx   Up     Enabled    Auto  (100F)    Enabled
 3    ---        1000tx   Up     Enabled          100-FDx   Enabled
 4    ---        1000tx   Up     Enabled    Auto  (1000F)   Enabled
 5    ---        1000tx   Up     Enabled    Auto  (100F)    Enabled
 6    ---        1000tx   Down   Enabled    Auto            Enabled
 7    ---        1000tx   Up     Enabled    Auto  (1000F)   Enabled
 8    ---        1000tx   Down   Enabled    Auto            Enabled
 9    ---        1000tx   Up     Enabled    Auto  (1000F)   Enabled
10    ---        1000tx   Up     Enabled          100-FDx   Enabled
11    ---        1000tx   Up     Enabled          10-FDx    Enabled
12    ---        1000tx   Up     Enabled    Auto (100F)     Enabled
---------------------- <COMMAND> ----------------------------------
[N]ext Page              Set [S]tatus     Set [F]low Control
[P]revious Page          Set [M]ode       [Q]uit to previous menu




Command>
```

Figure 13. Port Configuration Menu

The Port Configuration Menu displays the following columns of information about the status of the ports:

Port
The port number.

Trunk
The trunk group number. This column contains the number of the port trunk if the port is a member of a trunk. To configure a trunk, refer to Chapter 5, "Port Trunking" on page 57.

Type
The port type. The type for a 10/100/1000Base-TX port is 1000TX. The port type for an optional fiber optic SFP module is 1000BaseX.

Link
The status of the link between the port and the end node connected to the port. The possible values are:

Up - A link exists between the port and the end node.

Down - The port has not established a link with an end node.

Status
The current operating status of the port. The possible values are:

Enabled - The port is able to send and receive Ethernet frames. This is the default setting for all ports on the switch.

Disabled - The port has been manually disabled.

To change a port's status, see "Enabling and Disabling a Port" on page 53.

Mode
The port's speed and duplex mode setting. The possible values are:

Auto - The port is using Auto-Negotiation to set the operating speed and duplex mode. This is the default setting for all ports. The actual operating speed and duplex mode of the port are displayed in parentheses (for example, "Auto (1000F)" for 1000 Mbps full duplex mode).

If the speed and duplex mode were set manually on a port, mode will be one of the following:

10-HDx - 10 Mbps in half-duplex mode

100-HDx - 100 Mbps in half-duplex mode

10-FDx - 10 Mbps in full-duplex mode

100-FDx - 100 Mbps in full-duplex mode

1000-FDx - 1000 Mbps in full-duplex mode

1000-HDx - 1000 Mbps in half-duplex mode

To change a port's speed and duplex mode setting, see "Setting a Port's Speed and Duplex Mode" on page 54.

Flow Ctrl
Whether flow control is enabled on the port. Flow control is enabled by default. To disable flow control, refer to "Changing the Flow Control Setting" on page 56.

3. Type **Q** to select **Quit to previous menu**.

Enabling and Disabling a Port

This procedure enables and disables a port. You may want to disable a port and prevent packets from being forwarded if a problem occurs with the node or cable connected to the port. After the problem has been fixed, you can enable the port to resume normal operation. You can also disable an unused port to secure it from unauthorized connections. The default setting for a port is enabled.

To change the port's status, perform the following procedure:

1. From the Main Menu, type **B** to select **Basic Configuration**.

   The Basic Switch Configuration Menu is shown in Figure 4 on page 30

2. From the Basic Switch Configuration Menu, type **P** to select **Port Configuration**.

   The Port Configuration Menu is shown in Figure 13 on page 50.

3. Type **S** to select **Set Status**.

   The following prompt is displayed:

   ```
   Set Status->Enter port number>
   ```

4. Enter the number of the port you want to enable or disable. You can configure only one port at a time.

   The following prompt is displayed:

   ```
   Enable or Disable port n (E/D)>
   ```

5. Type **E** to enable the port or **D** to disable it. The default is enabled. A disabled port immediately stops forwarding all ingress and egress traffic until you enable it again.

   The display is refreshed to show the port's new status.

6. Type **Q** to select **Quit to previous menu** and save your changes.

Setting a Port's Speed and Duplex Mode

To change a port's speed or duplex mode, perform the following procedure:

1. From the Main Menu, type **B** to select **Basic Configuration**.

   The Basic Switch Configuration Menu is shown in Figure 4 on page 30

2. From the Basic Switch Configuration Menu, type **P** to select **Port Configuration**.

   The Port Configuration Menu is shown in Figure 13 on page 50.

3. Type **M** to select **Set Mode**.

   The following prompt is displayed:

   ```
   Set Mode -> Enter port number >
   ```

4. Enter the number of the port whose speed or duplex mode you want to change. You can configure only one port at a time.

   The following prompt is displayed:

   ```
   Enter new mode for port n (a/h/H/F/f/t/T)>
   ```

5. Enter the letter that corresponds to the desired speed and duplex mode setting for the port. The port settings are:

   a - Auto: The port uses Auto-Negotiation to set its speed and duplex mode. This is the default setting for all ports.

   h - 10 Mbps, half-duplex

   f - 10 Mbps, full-duplex

   H - 100 Mbps, half-duplex

   F - 100 Mbps, full-duplex

   t - 1000 Mbps, half-duplex

   T - 1000 Mbps, full-duplex

   When selecting a setting, note the following:

   - When a twisted pair port on the switch is set to Auto-Negotiation, the default setting, the end node should also be using Auto-Negotiation to prevent a duplex mode mismatch. A switch port using Auto-Negotiation defaults to half-duplex if it detects that the end node is not using Auto-Negotiation. This can result in a mismatch if the end node is operating at a fixed duplex mode of

full-duplex. To avoid this problem when connecting an end node with a fixed duplex mode of full-duplex to a switch port, disable Auto-Negotiation on the port and set the port's speed and duplex mode manually.

- Allied Telesyn does not recommend manually setting a 10/100/1000Base-T twisted pair port to either 1000 Mbps full duplex or 1000 Mbps half duplex. For 1000 Mbps operation, Allied Telesyn recommends setting a port to Auto-Negotiation.
- The only valid setting for an optional SFP port is Auto-Negotiation.

6. Type **Q** to select **Quit to previous menu** and save your changes.

Changing the Flow Control Setting

Flow control applies to ports operating in full-duplex mode. A switch port uses flow control to control the flow of ingress packets from its end node. A port using flow control issues a special frame, referred to as a PAUSE frame, as specified in the IEEE 802.3x standard, to stop the transmission of data from an end node. When a port needs to stop an end node from transmitting data, it issues this frame. The frame instructs the end node to cease transmission. The port continues to issue PAUSE frames until it is ready again to receive data from the end node.

To change the flow control setting on a port, perform the following procedure:

1. From the Main Menu, type **B** to select **Basic Configuration**.

   The Basic Switch Configuration Menu is shown in Figure 4 on page 30

2. From the Basic Switch Configuration Menu, type **P** to select **Port Configuration**.

   The Port Configuration Menu is shown in Figure 13 on page 50.

3. Type **S** to select **Set Status**.

   The following prompt is displayed:

   ```
   Set Flow Control -> Enter port number >
   ```

4. Enter the port number whose flow control setting you want to change. You can configure only one port at a time.

   The following prompt is displayed:

   ```
   Enable or Disable flow control for port <n> (E/D)>
   ```

5. Type **E** to enable flow control or **D** to disable it. The default is enabled.

   The display is refreshed to show the port's new flow control setting.

6. Type **Q** to select **Quit to previous menu** and save your changes.

Chapter 5

Port Trunking

This chapter provides information and procedures for creating a port trunk and contains the following sections:

Port Trunking Overview

Port trunking is an economical way for you to increase the bandwidth between two Ethernet switches. A port trunk is 2 to 8 ports that have been grouped together to function as one logical path. A port trunk increases the bandwidth between switches and is useful in situations where a single physical data link between switches is insufficient to handle the traffic load.

A port trunk always sends packets from a particular source to a particular destination over the same link within the trunk. A single link is designated for flooding broadcasts and packets of unknown destination.

Port Trunking Guidelines

Observe the following guidelines when creating a port trunk:

- A port trunk can consist of up to 8 ports.
- The switch can support up to 7 trunks.
- A port can belong to only one trunk at a time.
- The ports of a trunk must be of the same medium type. For example, they can be all twisted pair ports or all fiber optic ports.
- The speed, duplex mode, and flow control settings must be the same on all the ports in a trunk.
- The ports of a trunk must be members of the same VLAN. A port trunk cannot consist of ports from different VLANs.
- The ports of a trunk do not have to be consecutive.
- When you cable a trunk, the order of the connection should be maintained on both nodes. The lowest numbered port in a trunk on the switch should be connected to the lowest numbered port of the trunk on the other device, the next lowest numbered port on the switch should be connected to the next lowest numbered port on the other device, and so on.

  For example, assume that you are connecting a trunk between two AT-GS950 switches. On the first AT-GS950 switch you select ports 1 through 4 for a trunk. On the second AT-GS950 switch you select ports 6 through 9. To maintain the order of the port connections, connect port 1 on the first AT-GS950 switch to port 6 on the second AT-GS950 switch, port 2 to port 7, and so on.

- To avoid compatibility problems, Allied Telesyn recommends creating a port trunk only between AT-GS950 Series switches. A port trunk between an AT-GS950 Series switch and a device from another manufacturer might result in undesirable trunk behavior.

Creating a Port Trunk

This procedure explains how to create a port trunk.

> **Caution**
> Do not connect the cables to the ports on the switches until after you have configured the trunk with the management software. Connecting the cables before configuring the software creates a loop in your network topology, which can result in broadcast storms and poor network performance.

To create a port trunk, perform the following procedure:

1. From the Main Menu, type **A** to select **Advanced Switch Configuratio**n.

   The Advanced Switch Configuration Menu is shown in Figure 14.

```
AT-GS950/16 Local Management System
Main Menu -> Advanced Switch Configuration Menu

[V]LAN Management
[T]runk Configuration
Quality of [S]ervice Configuration
Port [M]irroring Configuration
802.x[X] Port Based Access Control Configuration
[Q]uit to previous menu




Command>
```

Figure 14. Advanced Switch Configuration Menu

2. From the Advanced Switch Configuration Menu, type **T** to select **Trunk Configuration**.

The Trunk Configuration Menu is shown in Figure 15.

```
AT-GS950/16 Local Management System
Advanced Switch Configuration -> Trunk Configuration Menu

Group     Status         Port Members          Trunk ID
-------   ------------- --------------------- ----------
   1      Disabled                                1
   2      Disabled                                2
   3      Disabled                                3
   4      Disabled                                4
   5      Disabled                                5
   6      Disabled                                6
   7      Disabled                                7



----------------------- <COMMAND> -----------------------------
[A]dd Trunk Member                      [S]et Trunk Status
[R]emove Trunk Member                   [Q]uit to previous menu


Command>
```

Figure 15. Trunk Configuration Menu

3. From the Trunk Configuration Menu, type **A** to select **Add Trunk Member**.

   The following prompt is displayed:

   ```
   Enter trunk group number>
   ```

4. Select a trunk group number from 1 to 7 and press Enter.

   The following prompt is displayed:

   ```
   Enter port members (up to 8 ports) for trunk n>
   ```

5. Enter the ports you want to include in the trunk and press Enter.

   You can specify the ports individually separated by commas (for example, 1,2,5), as a range of ports separated by a hyphen (for example, 2-4), or both (for example, 4,6,11-14).

6. Type **S** to select **Set Trunk Status**.

   The following prompt is displayed:

   ```
   Enter trunk group number>
   ```

7. Type the trunk group number and press Enter.

The following prompt is displayed:

```
Enable or Disable trunk group number n (E/D)>
```

8. Type **E** to enable the trunk.
9. Type **Q** to select **Quit to previous menu** and save your changes.

   The trunk is now operational on the switch.
10. Configure the port trunk on the other switch and connect the cables.

Modifying a Port Trunk

This procedure adds and removes ports from a port trunk.

> **Note**
> You should disconnect the cables from the ports of the trunk on the switch before modifying it. Adding or removing ports from a trunk without first disconnecting the cables can create loops in your network topology, which can cause broadcast storms and poor network performance.

To add or remove ports from a trunk, perform the following procedure:

1. From the Main Menu, type **A** to select **Advanced Switch Configuration**.

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 59.

2. From the Advanced Switch Configuration Menu, type **T** to select **Trunk Configuration**.

   The Trunk Configuration Menu is shown in Figure 15 on page 60.

3. To add ports to a port trunk, type **A** to select **Add Trunk Member**. To remove ports, type **R** to select **Remove Trunk Member**.

   The following prompt is displayed:

   ```
   Enter trunk group number>
   ```

4. Type the number of the trunk group you want to modify and press Enter.

   The following prompt is displayed:

   ```
   Enter port members (up to 8 ports) for trunk <n>>
   ```

5. Enter the ports you want to add or remove from the trunk and press Enter.

   You can specify the ports individually separated by commas (for example, 1,2,5), as a range of ports separated by a hyphen (for example, 2-4), or both (for example, 4,6,11-14).

6. Type **Q** to select **Quit to previous menu** and save your changes.

7. Modify the port trunk on the other switch and reconnect the cables.

Enabling and Disabling a Port Trunk

This procedure enables and disables a port trunk. Note the following before performing this procedure:

- Do not enable a port trunk until after you have configured the trunk on both switches.
- Do not connect the cables to the ports on the switches until after you have configured and enabled the trunk on both switches.

> **Note**
> If you are disabling a port trunk, be sure to first disconnect all cables from the ports of the trunk. Leaving the cables connected can create loops in your network topology because the ports of a disabled port trunk function as normal network ports, forwarding individual network traffic.

To enable or disable a port trunk, perform the following procedure:

1. From the Main Menu, type **A** to select **Advanced Switch Configuration**.

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 59.

2. From the Advanced Switch Configuration Menu, type **T** to select **Trunk Configuration**.

   The Trunk Configuration Menu is shown in Figure 15 on page 60.

3. From the Trunk Configuration Menu, type **S** to select **Set Trunk Status**.

   The following prompt is displayed:

   ```
   Enter trunk group number>
   ```

4. Type the number of the trunk group you want to enable or disable and press Enter.

   The following prompt is displayed:

   ```
   Enable or Disable trunk group number n (E/D)>
   ```

5. Type **E** to enable the trunk or **D** to disable it.

6. Type **Q** to select **Quit to previous menu** and save your changes.

Chapter 6

Port Mirroring

This chapter contains the procedure for setting up port mirroring. Port mirroring allows you to unobtrusively monitor the ingress and egress traffic on a port by having the traffic copied to another port. This chapter contains the following sections:

Port Mirroring Overview

The port mirroring feature allows you to unobtrusively monitor the ingress and egress traffic on a port on the switch by having the traffic copied to another switch port. By connecting a network analyzer to the port where the traffic is being copied to, you can monitor the traffic on the other port without impacting its performance or speed.

The port whose traffic you want to mirror is called the *mirrored port*. The port where the traffic will be copied to is called the *mirroring port*.

Observe the following guidelines when using this feature:

- ❒ You can mirror only one port at a time.
- ❒ The mirrored and mirroring ports must be on the same switch.
- ❒ This feature copies both the ingress and egress traffic of the mirrored port.
- ❒ The mirroring port cannot be used for normal Ethernet switching.

Configuring Port Mirroring

To set up port mirroring, perform the following procedure:

1. From the Main Menu, type **A** to select **Advanced Switch Configuration**.

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 59.

2. From the Advanced Switch Configuration Menu, type **M** to select **Port Mirroring Configuration**.

   The Port Mirroring Menu is shown in Figure 16.

```
AT-GS950/16 Local Management System
Advanced Switch Configuration -> Port Mirroring Configuration Menu

Mirroring Port    Mirrored Port    Status
---------------   --------------   ------
     2                 1          Disabled


----------------------- <COMMAND> -----------------------------
[S]et Mirroring Port
Set [M]irrored Port
[E]nable/Disable Port Mirroring
[Q]uit to previous menu


Command>
```

Figure 16. Port Mirroring Menu

3. Type **S** to select **Set Mirroring Port**.

   The following prompt is displayed:

   ```
   Set monitoring port-> Enter port number>
   ```

4. Type the number of the port where the network analyzer is connected and press Enter. You can specify only one port.

5. Type **M** to select **Set Mirrored Port**.

   The following prompt is displayed:

   ```
   Set monitored port-> Enter port number>
   ```

6. Type the number of the port whose ingress and egress traffic you want to monitor and press Enter. You can specify only one port.

7. Type **E** to select Enable/Disable Port Mirroring.

   The following prompt is displayed:

   ```
   Enable or Disable monitoring (E/D)>
   ```

8. Type **E** to enable port mirroring.

   You can now connect your data analyzer to the mirroring port.

9. Type **Q** to select **Quit to previous menu** and save your changes.

Disabling Port Mirroring

To disable port mirroring, perform the following procedure:

1. From the Main Menu, type **A** to select **Advanced Switch Configuration**.

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 59.

2. From the Advanced Switch Configuration Menu, type **M** to select **Port Mirroring Configuration**.

   The Port Mirroring Menu is shown in Figure 16 on page 67.

3. Type **E** to select **Enable/Disable Port Mirroring**.

   The following prompt is displayed:

   ```
   Enable or Disable monitoring (E/D)>
   ```

4. Type **D** to disable port mirroring.

   The port that was functioning as the mirroring port can now be used as a normal networking port.

5. Type **Q** to select **Quit to previous menu** and save your changes.

Chapter 7

Virtual LANs

This chapter contains the procedures for creating, modifying, and deleting port-based and tagged Virtual Local Area Networks (VLANs). This chapter contains the following sections:

VLAN Features

A Virtual Local Area Network (VLAN) is a logical grouping of devices on different physical LAN segments that allows users to communicate as if they were physically connected to a single LAN, independent of the physical configuration of the network.

With VLANs, you can segment your network and group end-nodes with related functions into their own separate, logical LAN segments. For example, the marketing personnel in you company may be spread throughout a building. Assigning marketing to a single VLAN allows marketing personnel to share resources and bandwidth as if they were connected to the same segment. The resources of other departments can be visible to the marketing VLAN members, accessible, or accessible only to specified individuals.

A few benefits of a VLAN architecture are described in the following sections.

Increased Performance

In traditional Layer 2 switched networks, broadcast packets are sent to each and every individual port. Grouping users into logical networks limits broadcast traffic to users performing similar functions or users within individual workgroups. High traffic, the danger of broadcast storms, router latency, and data collisions are significantly reduced, and the efficiency of the entire network is improved.

Improved Manageability

VLANs provide a fundamental improvement in the design, administration, and management of LANs. Before VLANs, physical changes to a network were made at the switch in the wiring closet.

For example, if an employee transferred to a new department, changing that employee's LAN segment assignment often required a physical wiring change at the switch.

As a software-base solution, VLANs eliminate the restriction of existing network design and cabling infrastructure and allow the centralized configuration of switches located in many different locations. VLAN memberships are changed quickly and efficiently from the management console rather than in a wiring closet.

Increased Security

VLANs provide additional security not available in a shared media network environment. Because a switched network only delivers frames to intended recipients, and only broadcast frames to other members of the VLAN, a network administrator can segment users requiring access to sensitive information into separate VLANs from the rest of the general user community.

VLANs can be used to control the flow of data in your network, since the traffic generated by an end-node in a VLAN is restricted to the other end-nodes in the same VLAN. In addition, VLANs can prevent data from flowing to unauthorized end-nodes.

Types of VLANs

The AT-GS950/16 and AT-GS950/24 switches support the following types of VLANs:

- Port-based VLANs
- Tagged VLANs

The VLANs are described in the following sections.

Port-based VLAN Overview

As explained in “VLAN Features” on page 72, a VLAN consists of a group of ports on one or more Ethernet switches that form an independent traffic domain. Traffic generated by the end nodes of a VLAN remains within the VLAN and does not cross over to the end nodes of other VLANs unless there is an interconnection device, such as a router or Layer 3 switch.

A port-based VLAN is a group of ports on a Gigabit Ethernet switch that form a logical Ethernet segment. Each port of a port-based VLAN can belong to only one VLAN at a time.

A port-based VLAN can have as many or as few ports as needed. The VLAN can consist of all the ports on an Ethernet switch, or just a few ports. A port-based VLAN also can span switches and consist of ports from multiple Ethernet switches.

Note
The AT-GS950/16 and AT-GS950/24 switches are preconfigured with one port-based VLAN, called the Default VLAN. All ports on the switch are members of this VLAN.

A port-based VLAN consists of the following parts:

- VLAN name
- VLAN Identifier
- Untagged ports
- Port VLAN Identifier

VLAN Name

To create a port-based VLAN, you must give it a name. The name should reflect the function of the network devices that are be members of the VLAN. Examples include Sales, Production, and Engineering.

VLAN Identifier

Every VLAN in a network must have a unique number assigned to it. This number is called the VLAN identifier (VID). This number uniquely identifies a VLAN in the switch and the network.

If a VLAN consists only of ports located on one physical switch in your network, you assign it a VID different from all other VLANs in your network.

If a VLAN spans multiple switches, then the VID for the VLAN on the different switches should be the same. The switches are then able to recognize and forward frames belonging to the same VLAN even though the VLAN spans multiple switches.

For example, if you had a port-based VLAN titled Marketing that spanned three AT-GS950 Series switches, you would assign the Marketing VLAN on each switch the same VID.

You can assign this number manually or allow the AT-S79 management software to do it automatically. If you allow the management software to do it automatically, it selects the next available VID. This is acceptable when you are creating a new, unique VLAN.

If you are creating a VLAN on a switch that will be part of a larger VLAN that spans several switch, you must assign the number yourself so that the VLAN has the same VID on all switches.

Untagged Ports

You need to specify which ports on the switch are to be members of a port-based VLAN. Ports in a port-based VLAN are referred to as *untagged ports* and the frames received on the ports as *untagged frames*. The names derive from the fact that the frames received on a port will not contain any information that indicates VLAN membership, and that VLAN membership will be determined solely by the port's PVID. (There is another type of VLAN where VLAN membership is determined by information within the frames themselves, rather than by a port's PVID. This type of VLAN is explained in "Tagged VLAN Overview" on page 80.)

A port on a switch can be an untagged member of only one port-based VLAN at a time. An untagged port cannot be assigned to two port-based VLANs simultaneously.

Port VLAN Identifier

Each port in a port-based VLAN must have a port VLAN identifier (PVID). The switch associates a frame to a port-based VLAN by the PVID assigned to the port on which the frame is received, and forwards the frame only to those ports with the same PVID. Consequently, all ports of a port-based VLAN must have the same PVID. Additionally, the PVID of the ports in a VLAN must match the VLAN's VID.

For example, if you were creating a port-based VLAN on a switch and you had assigned the VLAN the VID 5, the PVID for each port in the VLAN would need to be assigned the value 5.

Some switches assign the PVID value automatically when you assign an untagged port to a VLAN. However, with the AT-S79 management software you must perform this task manually.

Guidelines to Creating a Port-based VLAN

Below are the guidelines to creating a port-based VLAN.

- Each port-based VLAN must be assigned a unique VID. If a particular VLAN spans multiples switches, each part of the VLAN on the different switches should be assigned the same VID.
- A port can be an untagged member of only one port-based VLAN at a time.

- Each port must be assigned a PVID. This value must match the VLAN's VID and it must be the same for all the ports in a port-based VLAN. You must manually configure this value on a port after you assign the port to a VLAN. For instructions, refer to "Configuring the PVID of Untagged Ports" on page 87.
- A port-based VLAN that spans multiple switches requires a port on each switch where the VLAN is located to function as an interconnection between the switches where the various parts of the VLAN reside.
- If there are end nodes in different VLANs that need to communicate with each other, a router or Layer 3 switch is required to interconnect the VLANs.
- The switch can support up to a total of 256 port-based and tagged VLANs.

Drawbacks of Port-based VLANs

There are several drawbacks to port-based VLANs:

- It is not easy to share network resources, such as servers and printers, across multiple VLANs. A router or Layer 3 switch must be added to the network to provide a means for interconnecting the port-based VLANs. The introduction of a router into your network could create security issues from unauthorized access to your network.
- A VLAN that spans several switches requires a port on each switch for the interconnection of the various parts of the VLAN. For example, a VLAN that spans three switches would require one port on each switch to interconnect the various sections of the VLAN. In network configurations where there are many individual VLANs that span switches, many ports could end up being used ineffectively just to interconnect the various VLANs.

Port-based Example 1

Figure 17 illustrates an example of one AT-GS950/24 Gigabit Ethernet Switch with three port-based VLANs. (For purposes of the following examples, the Default VLAN is not shown.)

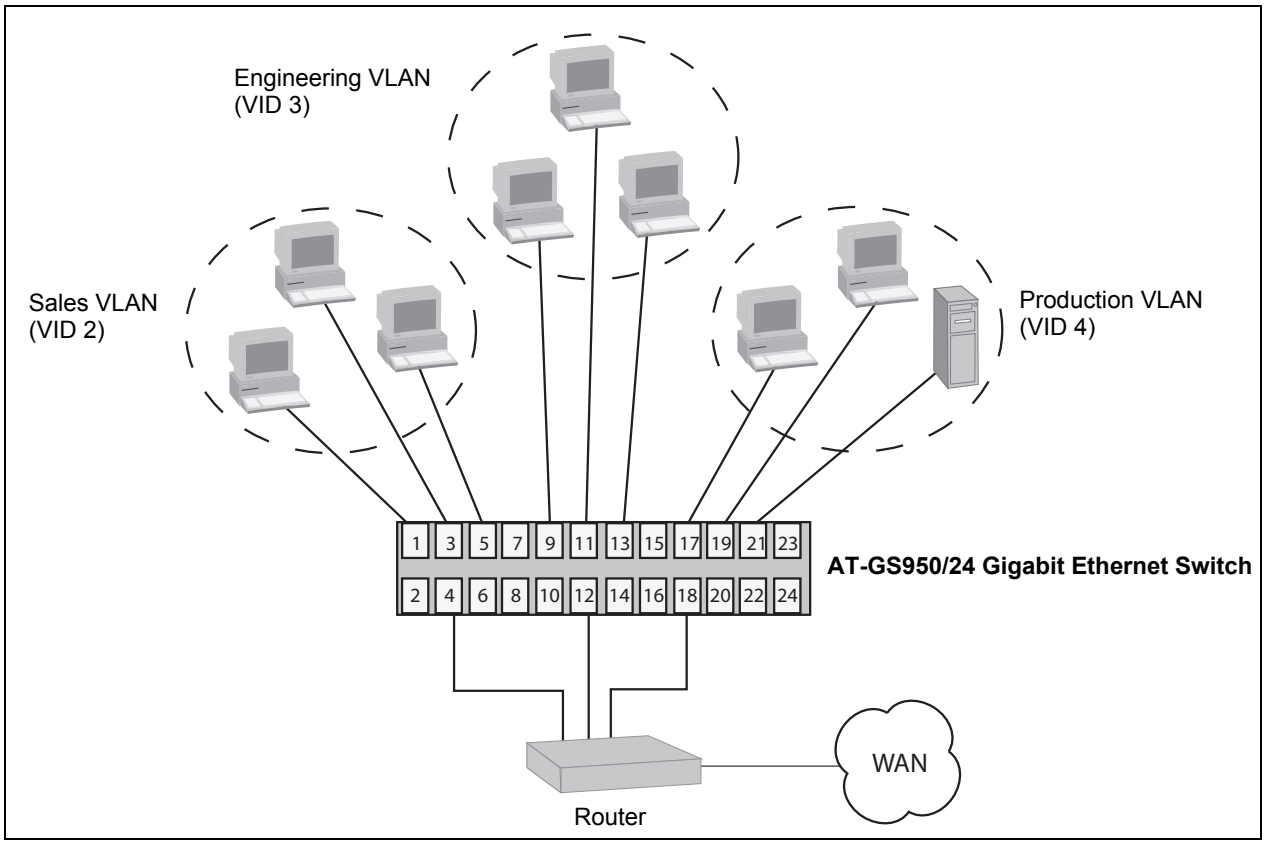


Figure 17. Port-based VLAN - Example 1

The table below lists the port assignments for the Sales, Engineering, and Production VLANs on the switch.

	Sales VLAN (VID 2)	**Engineering VLAN (VID 3)**	**Production VLAN (VID 4)**
AT-GS950/24 Switch	Ports 1, 3 - 5 (PVID 2)	Ports 9, 11 - 13 (PVID 3)	Ports 17 - 19, 21 (PVID 4)

Note the following about the example:

- Each VLAN has a unique VID, which is assigned when you create the VLANs.
- Each port's PVID value has been adjusted to equal the VID of its respective VLAN. In order for a port to be considered an untagged member of a VLAN, its PVID must equal the VID of the VLAN. This must be performed manually.

- Each VLAN has one port connected to the router. The router interconnects the various VLANs and functions as a gateway to the WAN.

Port-based Example 2

Figure 18 illustrates more port-based VLANs. In this example, Sales and Engineering VLANs span two AT-GS950/24 Gigabit Ethernet switches, while Production VLAN is limited to just one switch.

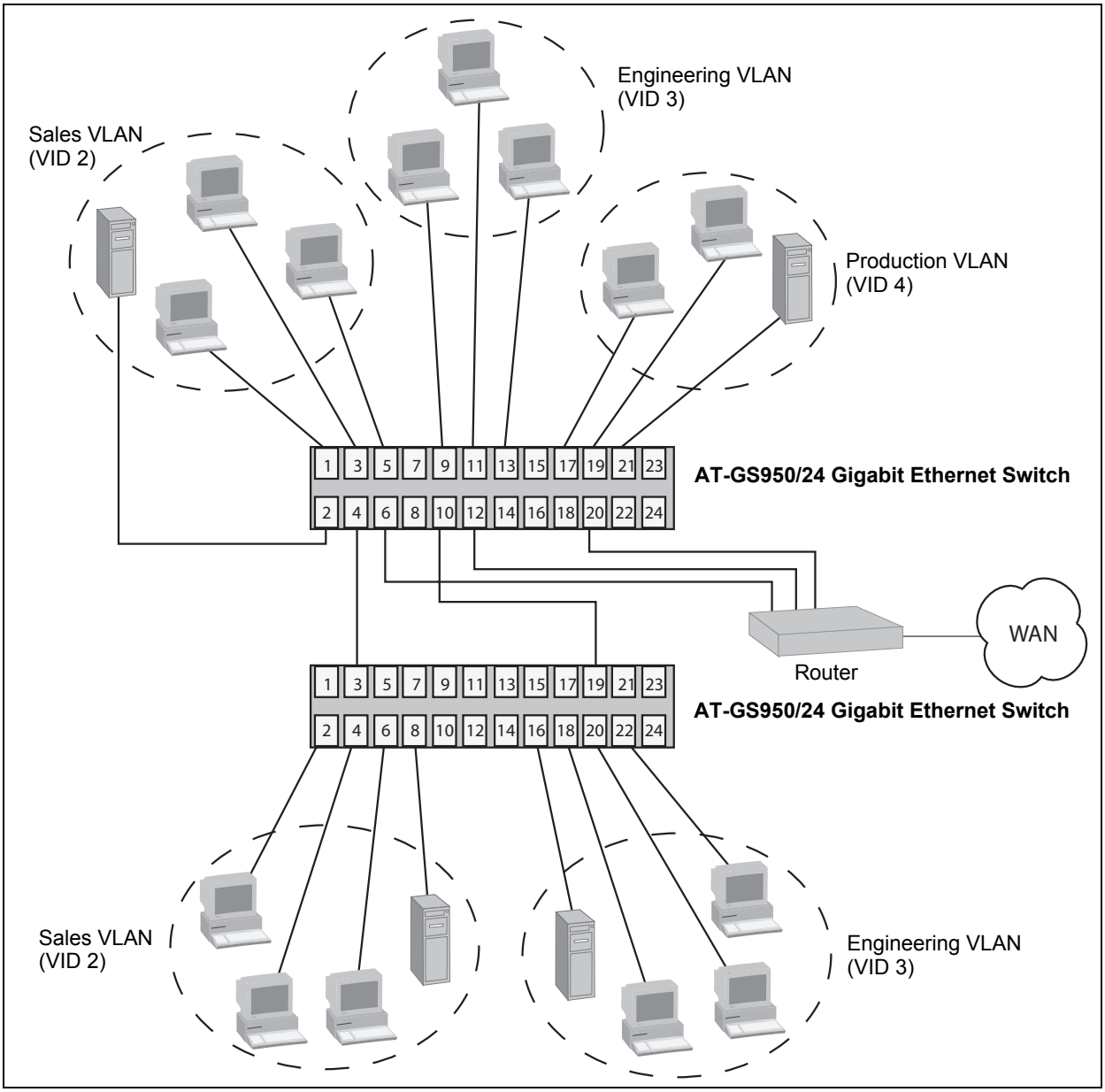


Figure 18. Port-based VLAN - Example 2

The table below lists the port assignments for the Sales, Engineering, and Production VLANs on the switches:

	Sales VLAN (VID 2)	**Engineering VLAN (VID 3)**	**Production VLAN (VID 4)**
AT-GS950/24 Switch (top)	Ports 1 - 6 (PVID 2)	Ports 9 - 13 (PVID 3)	Ports 17, 19 - 21 (PVID 4)
AT-GS950/24 Switch (bottom)	Ports 2 - 4, 6, 8 (PVID 2)	Ports 16, 18-20, 22 (PVID 3)	none

Note the following concerning the example:

- Sales VLAN - This VLAN spans both switches. It has a VID value of 2 and consists of six untagged ports on the top switch and five untagged ports on the bottom switch. The two parts of the VLAN are connected by a direct link from port 4 on the top switch to port 3 on the bottom switch. This direct link allows the two parts of the Sales VLAN to function as one logical LAN segment.

  Port 6 on the top switch connects to the router. This port allows the Sales VLAN to exchange Ethernet frames with the other VLANs and to access the WAN.

- Engineering VLAN - The workstations of this VLAN are connected to ports 9 to 13 on the top switch and ports 16, 18 to 20, and 22 on the bottom switch. Because this VLAN spans multiple switches, it needs a direct connection between its various parts to provide a communications path. This is provided in the example with a direct connection from port 10 on the top switch to port 19 on the bottom switch.

  This VLAN uses port 12 on the top switch as a connection to the router and the WAN.

- Production VLAN - This is the final VLAN in the example. It has the VLAN of 4 and its ports have been assigned the PVID also of 4. This VLAN does not require a direct connection to the bottom switch because its nodes are connected only to the top switch. However, it uses port 20 as a connection to the router.

Tagged VLAN Overview

The second type of VLAN supported by the AT-S79 management software is the *tagged VLAN*. VLAN membership in a tagged VLAN is determined by information within the frames that are received on a port. This differs from a port-based VLAN, where the PVIDs assigned to the ports determine VLAN membership.

The VLAN information within an Ethernet frame is referred to as a *tag* or *tagged header*. A tag, which follows the source and destination addresses in a frame, contains the VID of the VLAN to which the frame belongs (IEEE 802.3ac standard). This number, as explained earlier in “VLAN Identifier” on page 74, uniquely identifies each VLAN in a network.

When a switch receives a frame with a VLAN tag, referred to as a *tagged frame*, the switch forwards the frame only to those ports that share the same VID.

A port that receives and transmits tagged frames is referred to as a *tagged port*. Any network device connected to a tagged port must be IEEE 802.1Q-compliant. This is the standard that outlines the requirements and standards for tagging. The device must be able to process the tagged information on received frames and add tagged information to transmitted frames.

The benefit of a tagged VLAN is that the tagged ports can belong to more than one VLAN at one time. This can greatly simplify the task of adding shared devices to the network. For example, a server can be configured to accept and return packets from many different VLANs simultaneously.

Tagged VLANs are also useful where multiple VLANs span across switches. You can use one port per switch to connect all VLANs on the switch to another switch.

The IEEE 802.1Q standard describes how this tagging information is used to forward the traffic throughout the switch. The handling of frames tagged with VIDs coming into a port is straightforward. If the incoming frame’s VID tag matches one of the VIDs of a VLAN of which the port is a tagged member, the frame is accepted and forwarded to the appropriate ports. If the frame’s VID does not match any of the VLANs that the port is a member of, the frame is discarded.

The parts of a tagged VLAN are much the same as those for a port-based VLAN. They are:

- VLAN Name
- VLAN Identifier
- Tagged and Untagged Ports
- Port VLAN Identifier

Note
For explanations of VLAN name and VLAN identifier, refer back to "VLAN Name" on page 74 and "VLAN Identifier" on page 74.

Tagged and Untagged Ports

You need to specify which ports will be members of the VLAN. In the case of a tagged VLAN, the ports usually consist of both untagged and tagged ports. You specify which ports are tagged and which untagged when you create the VLAN.

An untagged port, whether a member of a port-based VLAN or a tagged VLAN, can be in only one VLAN at a time. However, a tagged port can be a member of more than one VLAN. A port can also be an untagged member of one VLAN and a tagged member of different VLANs simultaneously.

Port VLAN Identifier

As explained earlier in the discussion on port-based VLANs, the PVID of a port determines the VLAN where the port is an untagged member.

Because a tagged port determines VLAN membership by examining the tagged header within the frames that it receives, you could conclude that there is no need for a PVID. However, the PVID is used if a tagged port receives an untagged frame — a frame without any tagged information. The port forwards the frame based on the port's PVID. This is only in cases where an untagged frame arrives on a tagged port. Otherwise, the PVID of a tagged port is ignored.

Guidelines to Creating a Tagged VLAN

Below are the guidelines to creating a tagged VLAN.

- Each tagged VLAN must be assigned a unique VID. If a particular VLAN spans multiple switches, each part of the VLAN on the different switches must be assigned the same VID.
- A tagged port can be a member of multiple VLANs.
- An untagged port can be an untagged member of only one VLAN at a time.
- The switch can support up to a total of 256 port-based and tagged VLANs.

Tagged VLAN Example

Figure 19 illustrates how tagged ports can be used to interconnect IEEE 802.1Q-based products.

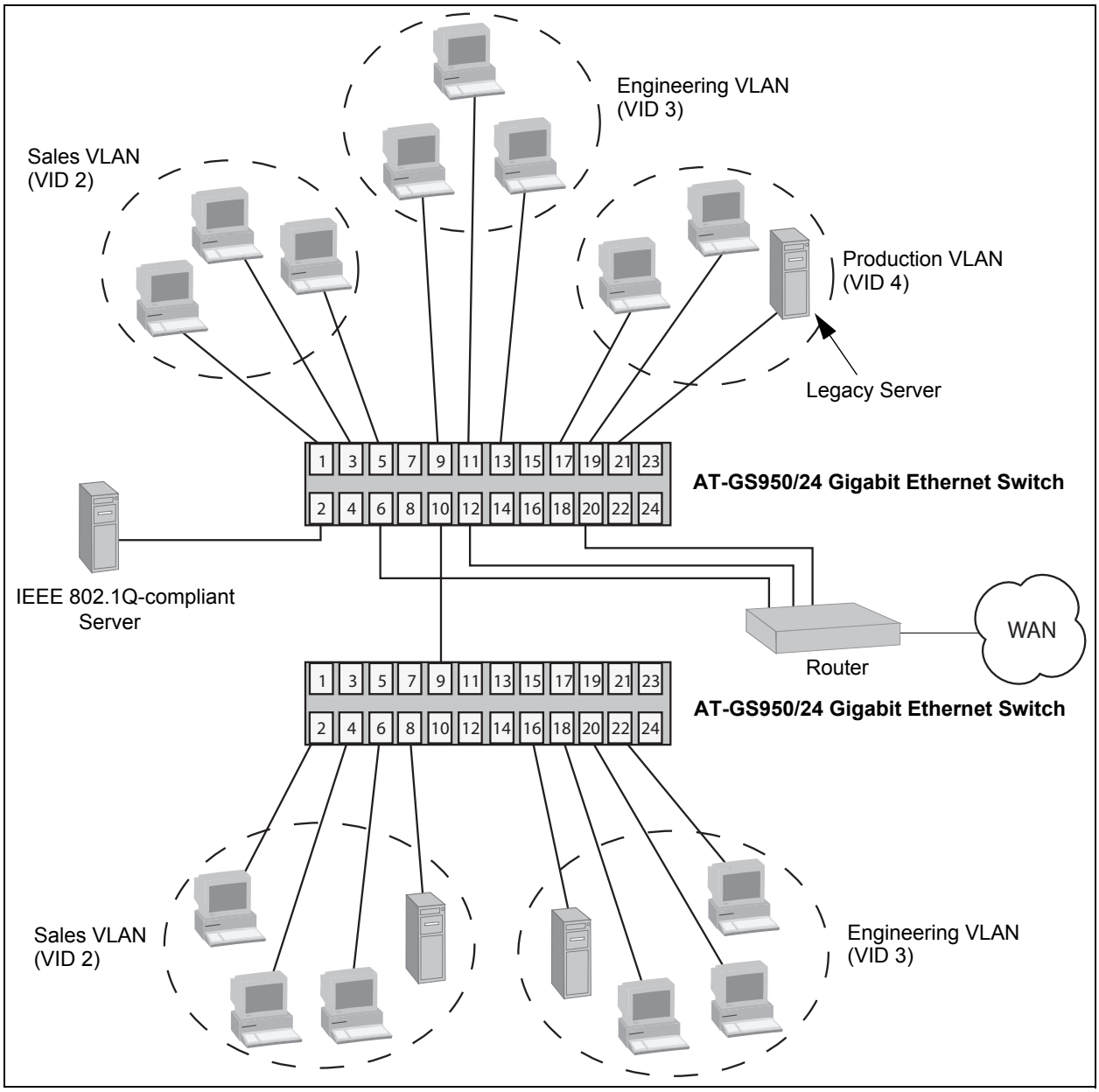


Figure 19. Example of a Tagged VLAN

The port assignments for the VLANs are as follows:

	Sales VLAN (VID 2)		**Engineering VLAN (VID 3)**		**Production VLAN (VID 4)**	
	Untagged Ports	Tagged Ports	Untagged Ports	Tagged Ports	Untagged Ports	Tagged Ports
AT-GS950/ 24 Switch (top)	1, 3, 5, 6 (PVID 2)	2, 10	9, 11 to 13 (PVID 3)	2, 10	17, 19 to 21 (PVID 4)	2
AT-GS950/ 24 Switch (bottom)	2, 4, 6, 8 (PVID 2)	9	16, 18, 20, 22 (PVID 3)	9	none	none

This example is nearly identical to the "Port-based Example 2" on page 78, but tagged ports have been added to simplify network implementation and management.

One of the tagged ports is port 2 on the top switch. This port has been made a tagged member of the three VLANs. It is connected to an IEEE 802.1Q-compliant server, meaning the server can handle frames from multiple VLANs. Now all three VLANs can access the server without going through a router or other interconnection device.

It is important to note that even though the server is accepting frames from and transmitting frames to more than one VLAN, data separation and security remain.

Two other tagged ports are used to simplify network design in the example. They are port 10 on the top switch and port 9 on the lower switch. These ports have been made tagged members of the Sales and Engineering VLANs so that they can carry traffic from both VLANs, simultaneously. These ports provide a common connection that enables different parts of the same VLAN to communicate with each other while maintaining data separation between VLANs.

In comparison, the Sales and Engineering VLANs in the "Port-based Example 2" on page 78 each had to have its own individual network link between the switches to connect the different parts of the VLANs. But with tagged ports, you can use one data link to carry data traffic from several VLANs, while still maintaining data separation and security. The tagged frames, when received by the switch, are delivered only to those ports that belong to the VLAN from which the tagged frames originated.

Creating a VLAN

This section contains the procedure for creating a new port-based or tagged VLAN. This procedure assigns the VLAN a name, a VID number, and the untagged and tagged member ports.

After you have performed this procedure, you must configure the untagged ports of the VLAN by adjusting their PVID values to match the virtual LAN's VID number. The PVID value of a port must match its virtual LAN's VID in order for a port to be considered an untagged member of the VLAN. This procedure is found in "Configuring the PVID of Untagged Ports" on page 87.

To create a VLAN, perform the following procedure:

1. From the Main Menu, type **A** to select **Advanced Switch Configuration**.

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 59.

2. From the Advanced Switch Configuration Menu, type **V** to select **VLAN Management**.

   The VLAN Management Menu is shown in Figure 20.

```
AT-GS950/16 Local Management System
Advanced Switch Configuration -> VLAN Management Menu

VLAN ID   VLAN Name                 VLAN Type
-------   ----------------------    ----------
   1      Default VLAN              Permanent
   3      Marketing                 Static




----------------------- <COMMAND> -----------------------------------
[N]ext Page             [C]reate VLAN          C[o]nfig VLAN Member
[P]revious Page         [D]elete VLAN          [S]et Port Config
[R]eset VLAN to Default                        [Q]uit to Previous Menu



Command>
```

Figure 20. VLAN Management Menu

3. From the VLAN Management Menu, type **C** to select **Create VLAN**.

   The VLAN Creation Menu is shown in Figure 21.

```
AT-GS950/16 Local Management System
VLAN Management -> VLAN Creation Menu

VLAN ID :
VLAN Name:

Port Member
-------------------------------------------------------------------------




------------------------- <COMMAND> ----------------------------------
Set VLAN [I]D/[I]ndex                S[e]lect Port Member
Set VLAN [N]ame                      [A]pply
[Q]uit to Previous Menu



Command>
```

Figure 21. VLAN Creation Menu

4. Type **I** to select **Set VLAN ID/Index**.

   The following prompt is displayed:

   ```
   Set VLAN ID->Enter VLAN ID>
   ```

   Note
   A VLAN must have a VID.

5. Enter a value from 2 to 4094 and press Enter.

6. Type **N** to select **Set VLAN Name**.

   The following prompt is displayed:

   ```
   Set VLAN Name -> Enter VLAN Name >
   ```

7. Type a name for the VLAN and press Enter. The VLAN name can contain up to 32 characters including spaces.

8. Type **S** to select **Select Port Number**.

The following prompt is displayed:

```
Enter port number >
```

9. Enter the untagged and tagged ports of the VLAN.

   You can specify the ports individually separated by commas, for example, 2,7,15, as a range of ports separated by a hyphen, for example, 2-4, or both, for example, 2-7,15,17.

10. When the VLAN is complete, type **A** to select **Apply** and apply the VLAN settings.

    The VLAN Management Menu is displayed again with information about the VLAN you just created. The VLAN is now active on the switch.

11. If the VLAN contains untagged ports, perform the next procedure, “Configuring the PVID of Untagged Ports” on page 87, to change the PVID of the untagged ports to match the virtual LAN’s VID.

Configuring the PVID of Untagged Ports

This procedure adjusts a port's VID value. The PVID value determines the VLAN in which the port is an untagged member. A port can be an untagged member of only one VLAN at a time. A port is an untagged member of the VLAN whose VID value matches its PVID.

The ports of a new VLAN are initially designated as tagged ports. Their PVID values retain their previous settings when they are assigned to a new VLAN. If you want the ports to function as untagged members of a new VLAN, you must change their PVID values to match the VID of the VLAN, as explained in this procedure.

You can also use this procedure to change the VLAN assignment of an untagged port. With this procedure you can move an untagged port from one VLAN to another by changing its PVID value.

To adjust the PVID value of a port, perform the following procedure:

1. From the Main Menu, type **A** to select **Advanced Switch Configuration**.

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 59.

2. From the Advanced Switch Configuration Menu, type **V** to select **VLAN Management**.

   The VLAN Management Menu is shown in Figure 20 on page 84.

3. Type **S** to select **Set Port Config**.

   The VLAN Port Configuration Menu is shown in Figure 20 on page 84

4. Type **V** to select **Set Port VID**.

   The following prompt is displayed:

   ```
   Set PVID->Enter port number
   ```

5. Type the number of the port whose PVID value you want to configure and press Enter. You can configure only one port at a time.

   The following prompt is displayed:

   ```
   Enter PVID for port n
   ```

6. Type the new PVID for the port and press Enter. The PVID should equal the VID of the VLAN where you want the port to be an untagged member.

Note
If you specify a PVID that does not correspond to any VIDs on the switch, the management software creates a new VLAN with a VID that equals the PVID. The VLAN is not assigned any name.

7. Repeat steps 4 through 6 to configure additional ports.
8. Type **Q** to select **Quit to previous menu** and save your changes.

Displaying the VLANs

To display a list of the port-based and tagged VLANs on the switch, perform the following procedure:

1. From the Main Menu, type **A** to select **Advanced Switch Configuration**.

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 59.

2. From the Advanced Switch Configuration Menu, type **V** to select **VLAN Management**.

   The VLAN Management Menu is shown in Figure 20 on page 84.

   The currently configured VLANs are displayed in a table with the following columns of information:

   VLAN ID
   The ID of the VLAN.

   VLAN Name
   The name of the VLAN.

   VLAN Type
   The type of VLAN, either permanent or static. Only the Default VLAN is permanent. All other port-based and tagged VLANs are static.

3. To view the ports of a VLAN, type **O** to select **Config VLAN Member**.

   The following prompt is displayed:

   ```
   Enter VLAN ID>
   ```

4. Enter the VID of the VLAN you want to view and press Enter.

The Config VLAN Member Menu is shown in Figure 22.

```
AT-GS950/16 Local Management System
VLAN Management -> Config VLAN Member

VLAN ID : 3   VLAN Name: Marketing


Port      Tagging
------------------------------------------------------------------------
  4       No
  5       No
  6       No
  7       No
  8       No
  24      Yes


----------------------- <COMMAND> -----------------------------------
[N]ext Page              [C]hange VLAN Name      [A]dd VLAN Member
[P]revious page          [R]emove VLAN Member    [Q]uit to Previous Menu



Command>
```

Figure 22. Config VLAN Member Menu

The menu displays the following information:

VLAN ID
The VID number of the VLAN.

VLAN Name
The name of the VLAN.

Port
The ports of the VLAN.

Tagging
Whether a port is a tagged or untagged member of the VLAN. An untagged port is designated with No and a tagged port with Yes.

The selections in this Config VLAN Member menu are explained in “Modifying a VLAN” on page 91.

Modifying a VLAN

This procedure allows you to perform the following functions:

- Change the name of a VLAN.
- Add or remove tagged ports from a VLAN.

Before performing this procedure, note the following:

- You cannot change the VID of a VLAN.
- You cannot add an untagged port to a VLAN with this procedure. That function requires changing a port's VID value, as explained in "Configuring the PVID of Untagged Ports" on page 87
- You cannot remove an untagged port from a VLAN with this procedure. To remove an untagged port from a VLAN, you must assign it as an untagged member of another VLAN by changing its PVID, as explained in "Configuring the PVID of Untagged Ports" on page 87.

To change the name of a VLAN or to add or remove tagged ports, perform the following procedure:

1. From the Main Menu, type **A** to select **Advanced Switch Configuration**.

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 59.

2. From the Advanced Switch Configuration Menu, type **V** to select **VLAN Management**.

   The VLAN Management Menu is shown in Figure 20 on page 84.

3. Type **O** to select **Config VLAN Member**.

   The following prompt is displayed:

   ```
   Enter VLAN ID >
   ```

4. Type the number of the VLAN you want to modify and press Enter.

   The Config VLAN Member menu is shown in Figure 22 on page 90.

5. To change the VLAN's name, do the following:

   a. Type **C** to select **Change VLAN Name**.

      The following prompt is displayed:

      ```
      Enter new VLAN name>
      ```

b. Type the new name for the VLAN and press Enter. A VLAN name can be up to 32 characters and can include spaces.

6. To add a tagged port to the VLAN, do the following:

   a. Type **A** for **Add Member** and press Enter.

      The following prompt is displayed:

      ```
      Add member->Enter port number >
      ```

   b. Enter the number of the port and press Enter. You can add more than one port at a time. You can specify the ports individually (i.e., 2,5,11), as a range (i.e., 4-7), or both (i.e., 2,5,11-15).

7. To remove a tagged port from the VLAN, do the following:

   a. Type **R** for **Remove Member** and press Enter.

      The following prompt is displayed:

      ```
      Delete number -> Enter port number >
      ```

   b. Enter the number of the tagged port you want to remove and press Enter. You can remove more than one port at a time. You can specify the ports individually (i.e., 2,5,11), as a range (i.e., 4-7), or both (i.e., 2,5,11-15).

8. Type **Q** to select **Quit to previous menu** and save your changes.

Deleting a VLAN

To delete a VLAN, perform the following procedure:

1. From the Main Menu, type **A** to select **Advanced Switch Configuratio**n.

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 59.

2. From the Advanced Switch Configuration Menu, type **V** to select **VLAN Management**.

   The VLAN Management Menu is shown in Figure 20 on page 84.

3. Type **D** to select **Delete VLAN**.

   The following prompt is displayed:

   ```
   Enter VLAN ID >
   ```

4. Type the VLAN ID of the VLAN you want to delete and press Enter. You can enter only one VID.

   Note
   The VLAN is immediately deleted with no confirmation prompt.

   Note
   You cannot delete the Default VLAN which has a VID of 1.

   The VLAN Management Menu is updated to show that the VLAN is deleted. The untagged ports of a deleted VLAN are automatically returned to the Default VLAN.

5. Type **Q** to select **Quit to previous menu** and save your changes.

Chapter 8

Quality of Service (QoS)

This chapter contains the procedures for configuring the Quality of Service (QoS) parameters of the switch. This chapter contains the following sections:

QoS Overview

When a port on an Ethernet switch becomes oversubscribed—its egress queues contain more packets than the port can handle in a timely manner—the port may be forced to delay the transmission of some packets, resulting in the delay of packets from reaching their destinations. A port may be forced to delay transmission of packets while it handles other traffic, and, in some situations, some packets destined to be forwarded to an oversubscribed port from other switch ports may be discarded.

Minor delays are often of no consequence to a network or its performance. But there are applications, referred to as delay or time sensitive applications, that can be impacted by packet delays. Voice transmission and video conferencing are two examples. If packets carrying data for either of these are delayed from reaching their destination, the audio or video quality may suffer.

This is where QoS can be of value. It allows you to manage the flow of traffic through a switch by having the switch ports give higher priority to some packets, such as delay sensitive traffic, over other packets. This is referred to as prioritizing traffic.

QoS actually consists of several different elements. The element supported by the AT-GS950/16 and AT-GS950/24 switches is called Class of Service (CoS). CoS applies primarily to tagged packets. As explained in “Tagged VLAN Overview” on page 80, a tagged packet contains information within it that specifies the VLAN to which the packet belongs.

A tagged packet can also contain a priority level. This priority level is used by network switches and other networking devices to know how important (delay sensitive) that packet is in comparison to other packets. Packets of a high priority are typically handled before packets of a low priority.

CoS, as defined in the IEEE 802.1p standard, has eight levels of priority. The priorities are 0 to 7, with 0 the lowest priority and 7 the highest.

When a tagged packet is received on a port on the switch, it is examined by the AT-S79 software for its priority. The switch software uses the priority to determine which egress priority queue the packet should be stored in on the egress port.

Each port on the AT-GS950/16 and AT-GS950/24 switches has four priority queues, 0 (low) to 3 (high). When a tagged packet enters a switch port, the switch responds by placing the packet into one of the queues according to the assignments shown in Table 2. A packet in a high priority egress queue is typically transmitted out a port sooner than a packet in a low priority queue.

Table 2. Default Mappings of IEEE 802.1p Priority Levels to Egress Port Priority Queues

IEEE 802.1p Traffic Class	AT-GS950 Series Egress Port Priority Queue
0	0
1	0
2	0
3	1
4	2
5	2
6	3
7	3

For example, a tagged packet with a priority tag of 6 is placed in the egress port's highest priority queue of 3, while a packet with a priority tag of 1 is placed in the lowest priority queue.

Note
QoS is disabled by default on the switch.

You can customize these priority-to-queue assignments using the AT-S79 management software. The procedure for changing the default mappings is found in "Mapping CoS Priorities to Egress Queues" on page 99. Note that because all ports must use the same priority-to-egress queue mappings, these mappings are applied at the switch level. They cannot be set on a per-port basis.

You can configure a port to completely ignore the priority levels in its tagged packets and instead use a temporary priority level assigned to the port. For instance, perhaps you decide that all tagged packets received on port 4 should be assigned a priority level of 5, regardless of the priority level in the packets themselves. The procedure for overriding priority levels is explained in "Configuring CoS" on page 102.

CoS relates primarily to tagged packets rather than untagged packets because untagged packets do not contain a priority level. By default, all untagged packets are placed in a port's Q0 egress queue, the queue with the lowest priority. But you can override this and instruct a port's untagged frames to be stored in a higher priority queue. The procedure for this is also explained in "Configuring CoS" on page 102.

One last thing to note is that CoS does not change the priority level in a tagged packet. The packet leaves the switch with the same priority it had when it entered. This is true even if you change the default priority-to-egress queue mappings.

The default setting for Quality of Service is disabled. When the feature is disabled, all tagged packets are stored in the lowest priority queue of a port.

Mapping CoS Priorities to Egress Queues

This procedure explains how to change the default mappings of CoS priorities to egress priority queues, shown in Table 2 on page 97. This is set at the switch level and applies to all ports. This procedure also enables and disables QoS.

To change the mappings, perform the following procedure:

1. From the Main Menu, type **A** to select **Advanced Switch Configuration**.

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 59.

2. From the Advanced Switch Configuration Menu, type **S** to select **Quality of Service Configuration**.

   The Quality of Service Configuration Menu is shown in Figure 23.

```
AT-GS950/16 Local Management System
Advanced Switch Configuration -> Quality of Service Configuration Menu

[T]raffic Class Configuration
[P]ort Priority Configuration
[Q]uit to previous menu









Command>
```

Figure 23. Quality of Service Configuration Menu

3. From the Quality of Service Configuration Menu, type **T** to select **Traffic Class Configuration**.

The Traffic Class Configuration Menu is shown in Figure 24.

```
AT-GS950/16 Local Management System
Quality of Service Configuration -> Traffic Class Configuration Menu

QoS Status : Disabled

Traffic Class     Queue
-------------     -----
     0              0
     1              0
     2              0
     3              1
     4              2
     5              2
     6              3               3 : Highest
     7              3               0 : Lowest

----------------------- <COMMAND> -----------------------------------
Set [S]tatus
Set [P]riority Queue
[Q]uit to previous Page


Command>
```

Figure 24. Traffic Class Configuration Menu

4. To enable or disable QoS, do the following:

   a. Type **S** to select **Set Status**.

      The following prompt is displayed:

      ```
      Enable or Disable QoS (E/D) >
      ```

   b. Type **E** to enable QoS or **D** to disable it. The default setting is disabled. When disabled, all tagged packets are stored in the lowest priority queue of a port.

5. To change the egress priority queue assignment of an 802.1p traffic class, do the following:

   a. Type **P** to select **Set Priority Queue**.

      The following prompt is displayed:

      ```
      Enter traffic class>
      ```

   b. Enter the traffic class whose egress priority queue you want to change. The range is 0 to 7. You can specify only one traffic class at a time.

The following prompt is displayed:

```
Enter queue for traffic class n>
```

c. Enter the new egress queue number for the traffic class. The range is 0 to 3. 0 is the lowest priority queue and 3 is the highest. You can specify only one egress queue.

6. Type **Q** to select **Quit to previous menu** and save your changes.

Configuring CoS

As explained in “QoS Overview” on page 96, a packet received on a port is placed it into one of four priority queues on the egress port according to the switch’s mapping of 802.1p priority levels to egress priority queues. The default mappings are shown in Table 2 on page 97.

You can override the mappings at the port level by assigning a different egress queue to a port. Note that this assignment is made on the ingress port and before the frame is forwarded to the egress port. Consequently, you need to configure this feature on the ingress port. For example, you can configure a switch port so that all ingress frames are stored in egress queue 3 of the egress port.

Note
The switch does not alter the original priority level in tagged frames. The frames leave the switch with the same priority level they had when they entered the switch.

To configure CoS for a port, perform the following procedure:

1. From the Main Menu, type **A** to select **Advanced Switch Configuration**.

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 59.

2. From the Advanced Switch Configuration Menu, type **S** to select **Quality of Service Configuration**.

   The Quality of Service Configuration Menu is shown in Figure 23 on page 99.

3. From the Quality of Service Configuration Menu, type **P** to select **Port Priority Configuration**.

The Port Priority Configuration Menu is shown in Figure 25.

```
AT-GS950/16 Local Management System
Quality of Service Configuration -> Port Priority Configuration Menu

QoS Status : Disabled

Port   Trunk   Queue   Override
----   -----   -----   --------
  1     ---     0      Disabled
  2     ---     0      Disabled
  3     ---     0      Disabled
  4     ---     0      Disabled
  5     ---     0      Disabled
  6     ---     0      Disabled
  7     ---     0      Disabled
  8     ---     0      Disabled
  9     ---     0      Disabled
 10     ---     0      Disabled
 11     ---     0      Disabled        3 : Highest
 12     ---     0      Disabled        0 : Lowest
---------------------- <COMMAND> ---------------------------------------
[N]ext Page             Set P[r]iority Queue     Set [T]runk Priority Queue
[P]revious Page         Set [O]verride Status    Set Trun[k] Override Status
[Q]uit to previous Page


Command>
```

Figure 25. Port Priority Configuration Menu

The columns in the menu display the following information:

Port
Displays the port number.

Trunk
Displays the trunk number if the port is a member of a trunk.

Queue
Displays the number of the queue where untagged packets received on the port are stored on the egress queue.

Override
Displays whether the priority level in ingress tagged frames is being used or not. If No, the override is deactivated and the port is using the priority levels contained within the frames to determine the egress queue. If Yes, the override is activated and the tagged packets are stored in the egress queue specified in the Queue column.

4. To configure a port that is not a member of a trunk, type **R** to select **Set Priority Queue**. To configure the ports of a port trunk, type **T** to select **Set Trunk Priority Queue**.

   The following prompt is displayed if you are configuring a port:

   ```
   Set Priority Queue->Enter port number>
   ```

   The following prompt is displayed if you are configuring a trunk:

   ```
   Enter trunk group number>
   ```

5. Enter the port or trunk number that you want to configure. You can configure only one port or trunk at a time.

   A prompt similar to the following is displayed:

   ```
   Enter queue for port n>
   ```

6. Enter the egress queue where the ingress untagged frames received on the port or trunk are to be stored on the egress port. The range is 0 (lowest) to 3 (highest). For example, if you enter 3 for queue 3, then all ingress untagged packets that are received on the port will be stored in egress queue 3 on the egress port. The default is 0. (If you perform Step 7 and override the priority level in ingress tagged packets, this also applies to those packets as well.)

7. To configure a tagged port or trunk so that the switch ignores the priority tag in ingress tagged frames, type **O** to select **Set Override Status** to configure a port or **K** to select **Set Trunk Override Status** to configure a trunk.

   The following prompt is displayed is you are configuring a port:

   ```
   Set Priority Queue->Enter port number>
   ```

   The following prompt is displayed if you are configuring a trunk:

   ```
   Enter trunk group number>
   ```

8. Enter the port or trunk number that you want to configure. You can configure only one port or trunk at a time.

   A prompt similar to the following is displayed:

   ```
   Enable or Disable override for port n (E/D)>
   ```

9. Type **E** to enable the override or **D** to disable it.

Note
The tagged information in a frame is not changed as the frame traverses the switch. A tagged frame leaves a switch with the same priority level that it had when it entered.

The default for this parameter is disabled, meaning that the priority level of tagged frames is determined by the priority level specified in the frames themselves.

Chapter 9

Rapid Spanning Tree Protocol (RSTP)

This chapter describes how to configure the Rapid Spanning Tree Protocol (RSTP) on the switch and includes the following sections:

RSTP Overview

The performance of a Ethernet network can be negatively impacted by the formation of a data loop in the network topology. A data loop exists when two or more nodes on a network can transmit data to each other over more than one data path. The problem that data loops pose is that data packets can become caught in repeating cycles, referred to as broadcast storms, that needlessly consume network bandwidth and can significantly reduce network performance.

RSTP prevents data loops from forming by ensuring that only one path exists between the end nodes in your network. Where multiple paths exist, this protocol places the extra paths in a standby or blocking mode, leaving only one main active path.

RSTP can also activate a redundant path if the main path goes down. So not only do these protocols guard against multiple links between segments and the risk of broadcast storms, but they can also maintain network connectivity by activating a backup redundant path in case a main link fails.

When a change is made to the network topology, such as the addition of a new bridge, a spanning tree protocol must determine whether there are redundant paths that must be blocked to prevent data loops, or activated to maintain communications between the various network segments. This is the process of convergence.

RSTP can complete a convergence in seconds, and so greatly diminishes the possible impact the process can have on your network.

At this time, only RSTP is available on the switch.

The RSTP implementation complies with the IEEE 802.1w standard. The following subsections provide a basic overview on how RSTP operates and define the different parameters that you can adjust.

Bridge Priority and the Root Bridge

The first task that bridges perform when a spanning tree protocol is activated on a network is the selection of a *root bridge*. A root bridge distributes network topology information to the other network bridges and is used by the other bridges to determine if there are redundant paths in the network.

A root bridge is selected by the *bridge priority* number, and sometimes the bridge's MAC address, also referred to as the bridge identifier. The bridge with the lowest bridge priority number in the network is selected as the root bridge. If two or more bridges have the same bridge priority number, of those bridges the one with the lowest MAC address is designated as the root bridge.

You can designate which switch on your network you want as the root bridge by giving it the lowest bridge priority number. You might also consider which bridge should function as the backup root bridge in the event you need to take the primary root bridge offline, and assign that bridge the second lowest bridge identifier number. You can change the bridge priority number for the switch.

The bridge priority has a range of 0X0000 to 0XF000 and is specified in multiples of 0x1000.

After the convergence process has completed, there is only one path between the switch and the root bridge. The active port on the switch through which the bridge is communicating with the root bridge is called the *root port*. Each switch in the spanning tree domain has a root port with the exception of the root bridge, which has no root port.

Designated Bridge and Designated Port

The switch that is directly connected to the root port of the switch is called the designated bridge. The port on the designated bridge that is connected to the switch's root port is called the designated port.

Path Costs and Port Costs

After the root bridge has been selected, the bridges must determine if the network contains redundant paths and, if one is found, they must select a preferred path while placing the redundant paths in a backup or blocking state.

If redundant paths exist, the bridges that are a part of the paths must determine which path will be the primary, active path, and which path(s) will be placed in the standby, blocking mode. This is accomplished by an determination of *path costs*. The path offering the lowest cost to the root bridge becomes the primary path and all other redundant paths are placed into blocking state.

Path cost is determined through an evaluation of *port costs*. Every port on a bridge participating in STP has a cost associated with it. The cost of a port on a bridge is typically based on port speed. The faster the port, the lower the port cost. The exception to this is the ports on the root bridge, where all ports have a port cost of 0.

Path cost is the sum of the port costs between a bridge and the root bridge.

Port cost also has an Auto-Detect feature. This feature allows spanning tree to automatically set the port cost according to the speed of the port, assigning a lower value for higher speeds. Auto-Detect is the default setting.

Table 3 lists the RSTP port costs with Auto-Detect.

Table 3. RSTP Auto-Detect Port Costs

Port Speed	Port Cost
10 Mbps	2,000,000
100 Mbps	200,000
1000 Mbps	20,000

Table 4 lists the RSTP port costs with Auto-Detect when the port is part of a port trunk.

Table 4. RSTP Auto-Detect Port Trunk Costs

Port Speed	No. of Ports/ Trunk	Port Cost
10/100/1000	2	10,000
10/100/1000	3	6,666
10/100/1000	4	5,000
10/100/1000	5	4,000
10/100/1000	6	3,333
10/100/1000	7	2,857
10/100/1000	8	2,500

You can override Auto-Detect and set the port cost manually. However, you must assign the same port cost to all ports that are members of a trunk.

Port Priority

If two paths have the same port cost, the bridges must select a preferred path. In some instances this can involve the use of the *port priority* parameter. This parameter is used as a tie breaker when two paths have the same cost.

The range for port priority, in hexadecimal format, is 0 to 240, with 240 being the highest priority. As with bridge priority, this range is broken into multiples of 16. To select a port priority for a port, you enter the desired value.

Table 5 lists the values. The default value is 0.

Table 5. Port Priority Value Increments

Port Priority	Port Priority
0	128
16	144
32	160
48	176
64	192
80	208
96	224
112	240

If two paths have the same port cost and the same priority, then the ports with the lowest port MAC addresses become the root ports of their respective bridges.

Hello Time and Bridge Protocol Data Units (BPDUs)

The bridges that are part of a spanning tree domain communicate with each other using a bridge broadcast frame that contains a special section devoted to carrying STP or RSTP information. This portion of the frame is referred to as the bridge protocol data unit (BPDU). When a bridge is brought online, it issues a BPDU in order to determine whether a root bridge has already been selected on the network, and if not, whether it has the lowest bridge priority number of all the bridges and should therefore become the root bridge.

The root bridge periodically transmits a BPDU to determine whether there have been any changes to the network topology and to inform other bridges of topology changes. The frequency with which the root bridge sends out a BPDU is called the *hello time*. This is a value that you can set in the AT-S79 management software. The interval is measured in seconds and the default is two seconds. Consequently, if an AT-9000/24 Gigabit Ethernet switch is selected as the root bridge of a spanning tree domain, it transmits a BPDU every two seconds.

Point-to-Point and Edge Ports

Part of the task of configuring RSTP is defining the port types on the bridge. This relates to the device(s) connected to the port. With the port types defined, RSTP can quickly reconfigure a network when a change in network topology is detected.

There are two possible selections:

- Point-to-point port
- Edge port

The default setting for the RSTP port point-to-point status is automatic. With the automatic setting, the point-to-point status is True of the port is operating in full-duplex mode. If the port is operating in half-duplex mode, then the point-to-point status is False.

Figure 26 illustrates two AT-GS950/24 switches that have been connected with one data link. With the link operating in full-duplex, the ports are point-to-point ports.

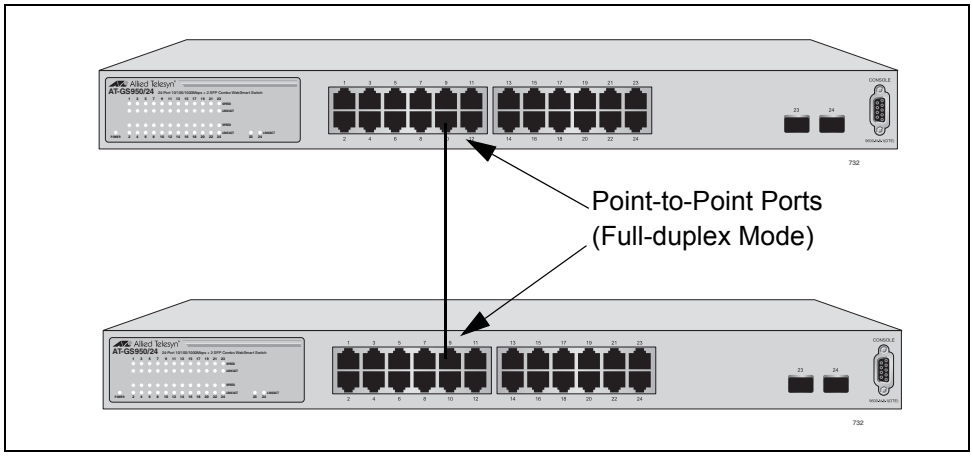


Figure 26. Point-to-Point Ports

If a port is operating in half-duplex mode and is not connected to any further bridges participating in STP or RSTP, then you need to manually define the port as an edge port. The default setting for the edge port status is False. You must manually configure this setting for each port. There is no automatic mode for the edge port setting. Figure 27 illustrates an edge port on an AT-GS950/24 switch. The port is connected to an Ethernet hub, which in turn is connected to a series of Ethernet workstations. This is an edge port because it is connected to a device operating at half-duplex mode and there are no participating STP or RSTP devices connected to it.

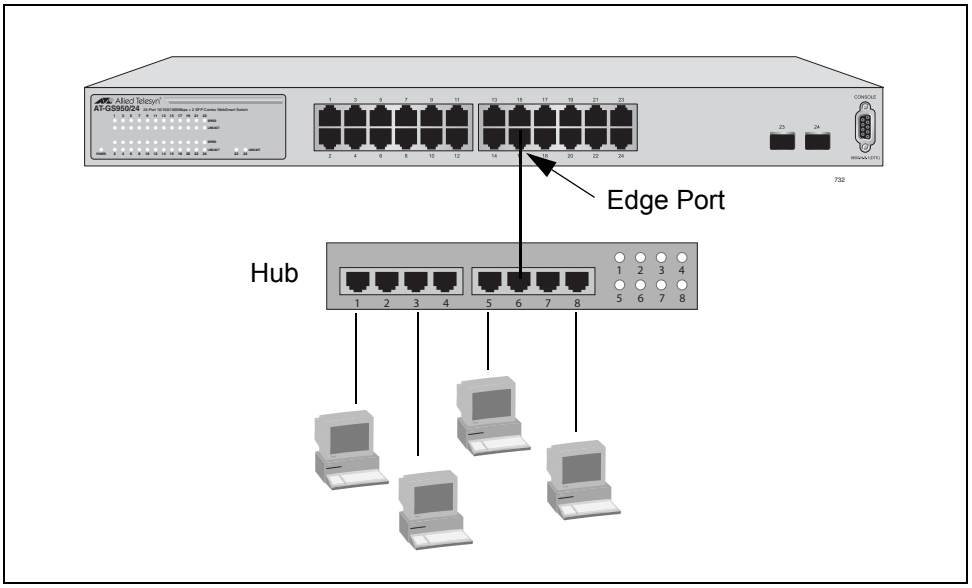


Figure 27. Edge Port

A port can be both a point-to-point and an edge port at the same time. Figure 28 illustrates a port functioning as both a point-to-point and edge port. You must manually configure the edge port status.

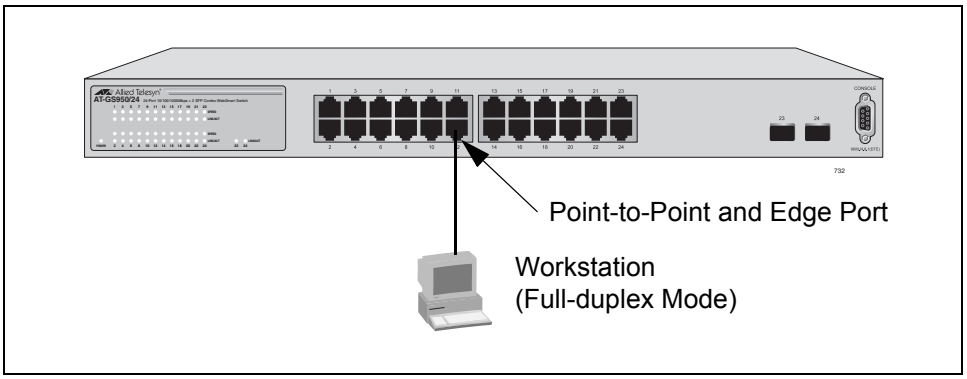


Figure 28. Point-to-Point and Edge Port

Determining whether a bridge port is point-to-point, edge, or both, can be a bit confusing. For that reason, do not change the default values for this RSTP feature unless you have a good grasp of the concept. In most cases, the default values work well.

Mixed STP and RSTP Networks

RSTP IEEE 802.1w is fully compliant with STP IEEE 802.1d. Your network can consist of bridges running both protocols. STP and RSTP in the same network can operate together to create a single spanning tree domain.

The switch monitors the traffic on each port for BPDU packets. When you set the switch to RSTP mode, all the ports operate in that mode and reject STP BPDU packets. When you set the switch to operate in STP-

compatible mode, the ports can receive either RSTP or STP BPDU packets.

Rapid Spanning Tree and VLANs

The spanning tree implementation in the AT-S79 management software is a single-instance spanning tree. The switch supports just one spanning tree. You cannot define multiple spanning trees.

The single spanning tree encompasses all ports on the switch. If the ports are divided into different VLANs, the spanning tree crosses the VLAN boundaries. This point can pose a problem in networks containing multiple VLANs that span different switches and are connected with untagged ports. In this situation, STP blocks a data link because it detects a data loop. This can cause fragmentation of your VLANs.

This issue is illustrated in Figure 29. Two VLANs, Sales and Production, span two switches. Two links consisting of untagged ports connect the separate parts of each VLAN. If RSTP is activated on the switches, one of the links is disabled. In the example, the port on the top switch that links the two parts of the Production VLAN is changed to the block state. This leaves the two parts of the Production VLAN unable to communicate with each other.

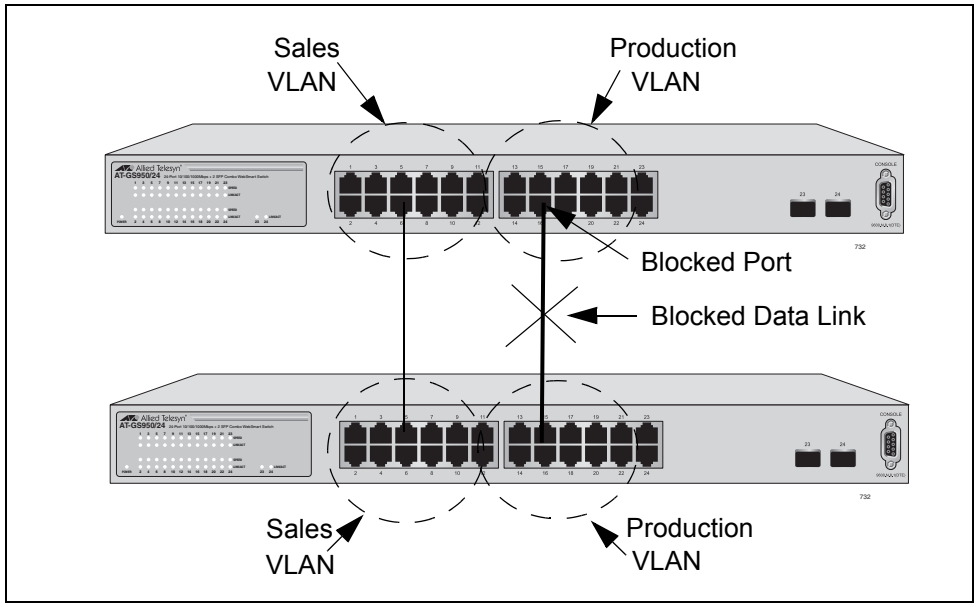


Figure 29. VLAN Fragmentation

You can avoid this problem by not activating rapid spanning tree or by connecting VLANs using tagged port members instead of untagged ports. (For information on tagged and untagged ports, refer to Chapter 7, “Virtual LANs” on page 71.)

Enabling or Disabling RSTP

To enable or disable RSTP, perform the following procedure:

1. From the Main Menu, type **B** to select **Basic Switch Configuration**.

   The Basic Switch Configuration Menu is shown in Figure 4 on page 30.

2. From the Basic Switch Configuration Menu, type **S** to select **Rapid Spanning Tree Configuration**.

   The Rapid Spanning Tree Configuration Menu is shown in Figure 30.

```
AT-GS950/16 Local Management System
Basic Switch Configuration -> Rapid Spanning Tree Configuration Menu

Global RSTP Status: Disabled          Protocol Version: RSTP

Root Port:       0                    Time Since Topology Change: 118  Sec.
Root Path Cost:  0                    Topology Change Count:      1

Designated Root: 8000 00C08F1211BB    Bridge ID:             8000 010203AABB04
Hello Time:      2 Sec.               Bridge Hello Time:     2 Sec.
Maximum Age:     20 Sec.              Bridge Maximum Age:    20 Sec.
Forward Delay:   15 Sec.              Bridge Forward Delay:  15 Sec.

----------------------- <COMMAND> -----------------------------
[E]nable/Disable Global RSTP          Set Bridge [F]orward Delay
Set RSTP Protocol [V]ersion           RSTP [B]asic Port Configuration
Set Bridge [P]riority                 RSTP [A]dvanced Port Configuration
Set Bridge [H]ello Time               Topology [I]nformation
Set Bridge [M]aximum Age              [Q]uit to previous menu


Command>
```

Figure 30. RSTP Configuration Menu

The RSTP menu allows you to configure RSTP as well as to view the current settings and contains the following items of information in the middle portion:

Root Port
The active port on the switch that is communicating with the root bridge. If the switch is the root bridge for the LAN, then there is no root port and the root port parameter will be 0.

Root Path Cost
The sum of all the root port costs of all the bridges between the

switch's root port and the root bridge including the switch's root port cost.

Time Since Topology Change
The time in seconds since the last topology change took place. When RSTP detects a change to the LAN's topology or when the switch is rebooted, this parameter is reset to 0 seconds and begins incrementing until the next topology change is detected.

Topology Change Count
An integer that reflects the number of times RSTP has detected a topology change on the LAN since the switch was initially powered on or rebooted.

The following parameters refer to the designated root bridge:

Designated Root
This parameter includes two fields: the root bridge priority and the MAC address of the root bridge. For example, 1000 00C08F1211BB shows the root bridge priority as 1000, and 00C08F1211BB as the MAC address.

Hello Time
The hello time. See "Hello Time and Bridge Protocol Data Units (BPDUs)" on page 111. This parameter affects only the root bridge.

Maximum Age
The maximum amount of time that BPDUs are stored before being deleted on the root bridge.

Forward Delay
The time interval between generating and sending configuration messages by the root bridge.

The following parameters refer to the switch.

Bridge ID
The MAC address of the bridge. The bridge identifier is use as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority. You cannot change this setting.

Bridge Hello Time
This is the time interval between generating and sending configuration messages by the bridge. This parameter is active only when the switch is the root bridge.

Bridge Maximum Age
The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge.

Bridge Forward Delay
This is the time interval between generating and sending configuration messages by the bridge.

3. Type **E** to select **Enable/Disable Global RSTP**.

   The following prompt is displayed:

   ```
   Enable or Disable Global RSTP (E/D)>
   ```

4. Type **E** to enable RSTP or **D** to disable RSTP.

Configuring the RSTP Bridge Settings

To configure the RSTP bridge settings, perform the following procedure:

1. From the Main Menu, type **B** to select **Basic Switch Configuration**.

   The Basic Switch Configuration Menu is shown in Figure 4 on page 30.

2. From the Basic Switch Configuration Menu, type **S** to select **Rapid Spanning Tree Configuration**.

   The Rapid Spanning Tree Configuration Menu is shown in Figure 30 on page 115.

3. Type **P** to select **Set Bridge Priority**.

   The following prompt is displayed:

   ```
   Enter bridge priority>
   The value is in the range from 0x0000 to 0xF000 and in
   increments of 0x1000.
   ```

   The priority number for the bridge, in hexadecimal format. This number is used to determine the root bridge for RSTP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, that is, the lowest of all the other bridges, then the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes offline, the bridge with the lowest priority number automatically takes over as the root bridge. This parameter can be from 0X0000 to 0XF000, with 0XF000 being the highest priority.

   The bridge priority is shown as the first field in the “Designated Root” and “Bridge ID” parameters.

4. Enter a number for the bridge priority.

5. Type **H** to select **Set Bridge Hello Time**.

   The following prompt is displayed:

   ```
   Enter bridge hello time>
   ```

   This is the time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

6. Enter a number for the bridge hello time.

7. Type **M** to select **Set Bridge Maximum Age**.

The following prompt is displayed:

```
Enter bridge maximum age>
```

The bridge maximum age is the length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default value 20, all bridges delete current configuration messages after 20 seconds. This parameter can be from 6 to 40 seconds.

When you select a value for maximum age, observe the following rules:

MaxAge must be greater than (2 x (HelloTime + 1)).

MaxAge must be less than (2 x (ForwardingDelay - 1)).

Note
The aging time for BPDUs is different from the aging time used by the MAC address table.

8. Enter a number for the bridge maximum age.
9. Type **F** to select **Set Bridge Forward Delay**.

   The following prompt is displayed:

   ```
   Enter bridge forward delay>
   ```

   The bridge forwarding delay is the waiting period in seconds before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, resulting in network loops. The range is 4 to 30 seconds. The default is 15 seconds.

10. Enter a number for the bridge forward delay, between 4 and 30 seconds.

Configuring STP Compatibility

Choosing an RSTP protocol version allows you to determine if the switch ports will operate in RSTP-only mode or are STP-compatible. This setting applies to all of the ports; you cannot set this on a per-port basis.

To configure the STP compatibility, perform the following procedure:

1. From the Main Menu, type **B** to select **Basic Switch Configuration**.

   The Basic Switch Configuration Menu is shown in Figure 4 on page 30.

2. From the Basic Switch Configuration Menu, type **S** to select **Rapid Spanning Tree Configuration**.

   The Rapid Spanning Tree Configuration Menu is shown in Figure 30 on page 115.

3. Type **V** to select **Set RSTP Protocol Version**.

   The following prompt is displayed:

   ```
   Set RSTP protocol version (S/R)>
   ```

4. Type **S** to make the ports STP-compatible, or **R** to make the ports operate only in RSTP mode.

Configuring RSTP Port Settings

This section contains the following topics:

Configuring the Basic RSTP Port Settings

To configure the basic RSTP port settings, perform the following procedure:

1. From the Main Menu, type **B** to select **Basic Switch Configuration**.

   The Basic Switch Configuration Menu is shown in Figure 4 on page 30.

2. From the Basic Switch Configuration Menu, type **S** to select **Rapid Spanning Tree Configuration**.

   The Rapid Spanning Tree Configuration Menu is shown in Figure 30 on page 115.

3. From the Rapid Spanning Tree Configuration Menu, type **B** to select **RSTP Basic Port Configuration**.

   The RSTP Basic Port Configuration menu is shown in Figure 31.

```
AT-GS950/16 Local Management System
Rapid Spanning Tree Configuration -> RSTP Basic Port Configuration

Port  Trunk   Link  State        Role       Priority    Path Cost    STP Status
----  -----   ----  ----------   --------- ---------------------------
1     ---     Up    Forwarding   Disabled    128        200000       Disabled
2     ---     Down  Forwarding   Disabled    128        200000       Enabled
3     ---     Up    Forwarding   Root        128        200000       Enabled
4     ---     Down  Forwarding   Disabled    128        200000       Enabled
5     ---     Down  Forwarding   Disabled    128        200000       Enabled
6     ---     Down  Forwarding   Disabled    128        200000       Enabled
7     ---     Down  Forwarding   Disabled    128        200000       Enabled
8     ---     Down  Forwarding   Disabled    128        200000       Enabled
9     ---     Down  Forwarding   Disabled    128        20000        Enabled
10    ---     Down  Forwarding   Disabled    128        20000        Enabled
11    ---     Down  Forwarding   Disabled    128        20000        Enabled
12    ---     Down  Forwarding   Disabled    128        20000        Enabled
----------------------------- <COMMAND> ---------------------------------
[N]ext Page                                    Set Path [C]ost
[P]revious Page                                Set Port STP [S]tatus
Set Port Pr[i]ority                            [Q]uit to previous menu

Command>
```

Figure 31. RSTP Basic Port Configuration Menu

4. Type **I** to select **Set Port Priority**.

   The following prompt is displayed:

   ```
   Select port number to be changed>
   Port number is in range from 1 to 9, 0 to set all ports
   ```

5. Enter the number of the port you want to change, or type 0 (zero) to apply the settings to all ports on the switch.

   The following prompt is displayed:

   ```
   Enter priority for port n>
   ```

   This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0 to 240 in increments of 16. The default value is 8 (priority value 128). For a list of the increments, refer to Table 5 on page 111.

   Note
   If two or more ports have the same cost and priorities, then the port with the lowest MAC address becomes the forwarding port.

6. Enter a number for the priority.

7. Type **C** to select **Set Path Cost**.

   The following prompt is displayed:

   ```
   Select port number to be changed>
   Port number is in range from 1 to 9, 0 to set all ports
   ```

8. Enter the number of the port you want to change, or type 0 (zero) to apply the settings to all ports on the switch.

   The following prompt is displayed:

   ```
   Enter path cost for port n>
   ```

   The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN.The range is from 0 to 240, with 240 being the highest priority. For a list of the increments, refer to Table 5 on page 111.

   The default setting is based on the Auto-Detect Port Cost feature, which sets port cost depending on the speed of the port. The default values are shown in Table 3 on page 110.

9. Enter a number for the path cost.

10. Type **S** to select **Set Port STP Status**.

```
Select port number to be changed>
Port number is in range from 1 to 9, 0 to set all ports
```

This parameter enables or disables RSTP on a specified port or a group of ports in a trunk.

11. Enter the number of the port you want to change, or type 0 (zero) to apply the settings to all ports on the switch.

    The following prompt is displayed:

    ```
    Enable or Disable STP for port n (E/D)>
    ```

12. Type **E** to enable or **D** to disable STP on the port.

Configuring the Advanced RSTP Port Settings

To configure the advanced RSTP port settings, perform the following procedure:

1. From the Main Menu, type **B** to select **Basic Switch Configuration**.

   The Basic Switch Configuration Menu is shown in Figure 4 on page 30.

2. From the Basic Switch Configuration Menu, type **S** to select **Rapid Spanning Tree Configuration**.

   The Rapid Spanning Tree Configuration Menu is shown in Figure 30 on page 115.

3. From the Rapid Spanning Tree Configuration Menu, type **A** to select **RSTP Advanced Port Configuration**.

The RSTP Advanced Port Configuration menu is shown in Figure 31.

```
AT-GS950/16 Local Management System
Rapid Spanning Tree Configuration -> RSTP Advanced Port Configuration

Port  Trunk  Link  State       Role     Admin/OperEdge  Admin/OperPtoP  Migrat
----  -----  ----  ----------  ---------------------------------------
 1    ---    Down  Forwarding  Disabled  False/False    Auto/False      Init.
 2    ---    Down  Forwarding  Disabled  False/False    Auto/False      Init.
 3    ---    Down  Forwarding  Disabled  False/False    Auto/False      Init.
 4    ---    Down  Forwarding  Disabled  False/False    Auto/False      Init.
 5    ---    Down  Forwarding  Disabled  False/False    Auto/False      Init.
 6    ---    Down  Forwarding  Disabled  False/False    Auto/False      Init.
 7    ---    Down  Forwarding  Disabled  False/False    Auto/False      Init.
 8    ---    Down  Forwarding  Disabled  False/False    Auto/False      Init.
 9    ---    Down  Forwarding  Disabled  False/False    Auto/False      Init.
10    ---    Down  Forwarding  Disabled  False/False    Auto/False      Init.
11    ---    Down  Forwarding  Disabled  False/False    Auto/False      Init.
12    ---    Down  Forwarding  Disabled  False/False    Auto/False      Init.
------------------------------ <COMMAND> --------------------------------
[N]ext Page                                  Set Port P-[t]o-P Status
[P]revious Page                              Restart Port [M]igration
Set Port [E]dge Status                       [Q]uit to previous menu

Command>
```

Figure 32. RSTP Advanced Port Configuration Menu

4. Type **E** to select **Edge Status**.

   The following prompt is displayed:

   The following prompt is displayed:

   ```
   Select port number to be changed>
   Port number is in range from 1 to 9, 0 to set all ports
   ```

5. Enter the number of the port you want to change, or type 0 (zero) to apply the settings to all ports on the switch.

   The following prompt is displayed:

   ```
   Set edge port for port n >(T/F)>
   ```

   This parameter defines whether the port is functioning as an edge port. The possible settings are True and False. For an explanation of this parameter, refer to “Point-to-Point and Edge Ports” on page 111.

6. Enter **T** for True or **F** for False to change the Admin/OperEdge status.

7. Type **P** to select **P-to-P Status**.

The following prompt is displayed:

```
Select port number to be changed>
Port number is in range from 1 to 9, 0 to set all ports
```

8. Enter the number of the port you want to change, or type 0 (zero) to apply the settings to all ports on the switch.

   The following prompt is displayed:

   ```
   Set point-to-point for port n >(A/T/F)
   ```

   This parameter defines whether the port is functioning as a point-to-point port. The possible settings are Auto, True, and False. For an explanation of this parameter, refer to "Point-to-Point and Edge Ports" on page 111.

9. Enter **A** for Auto, **T** for True, or **F** for False, according to the operating status your network requires, following the guidelines in Table 6.

Table 6. RSTP Point-to-Point Status

Admin	Operation	Port Duplex Operation
Auto	True	Full
	False	Half
True	True	Full or Half
False	False	Full or Half

10. Type **M** to select **Restart Port Migration**.

    The following prompt is displayed:

    ```
    Select port number to be changed>
    ```

11. Enter the number of the port you want to change.

    The following prompt is displayed:

    ```
    Restart the protocol migration process for port n? (Y/N)
    ```

    This parameter resets an RSTP port, allowing it to send RSTP BPDUs. When an RSTP bridge receives STP BPDUs on an RSTP port, the port transmits STP BPDUs. The RSTP port continues to transmit STP BPDUs indefinitely.

12. Enter **T** for True or **F** for False.

Displaying the RSTP Topology

To display the RSTP topology, perform the following procedure:

1. From the Main Menu, type **B** to select **Basic Switch Configuration**.

   The Basic Switch Configuration Menu is shown in Figure 4 on page 30.

2. From the Basic Switch Configuration Menu, type **S** to select **Rapid Spanning Tree Configuration**.

   The Rapid Spanning Tree Configuration Menu is shown in Figure 30 on page 115.

3. From the Rapid Spanning Tree Configuration Menu, type **I** to select **Topology Information**.

   The Topology Information menu is shown in Figure 31.

```
AT-GS950/16 Local Management System
Rapid Spanning Tree Configuration -> Designated Topology Information

 PortTrunk Link  Desig. Root        Desig. Cost  Desig. Bridge    Desig. Port
 --------- ----  ------------------------------------------------------------
 1         Up    8000 00c08f1211bb  0            8000 00c08f1211bb 00 00
 2         Down  8000 00c08f1211bb  0            8000 00c08f1211bb 00 00
 3         Up    8000 000c46aa7fal  200000       8000 003084000000 00 03
 4         Down  8000 00c08f1211bb  0            8000 00c08f1211bb 00 00
 5         Down  8000 00c08f1211bb  0            8000 00c08f1211bb 00 00
 6         Down  8000 00c08f1211bb  0            8000 00c08f1211bb 00 00
 7         Down  8000 00c08f1211bb  0            8000 00c08f1211bb 00 00
 8         Down  8000 00c08f1211bb  0            8000 00c08f1211bb 00 00
 9         Down  8000 00c08f1211bb  0            8000 00c08f1211bb 00 00
10         Down  8000 00c08f1211bb  0            8000 00c08f1211bb 00 00
11         Down  8000 00c08f1211bb  0            8000 00c08f1211bb 00 00
12         Down  8000 00c08f1211bb  0            8000 00c08f1211bb 00 00

--------------------------------- <COMMAND> ---------------------------------
[N]ext Page                  [P]revious Page      [Q]uit to previous menu

Command>
```

Figure 33. Topology Information Menu

This menu displays the following information about the ports:

Trunk
The trunk of which the port is a member.

Link
Whether the link on the port is up or down.

Desig. Root
The designated root bridge is the switch that is directly connected to the local switch. The MAC address of the designated root bridge is displayed. In the network topology, the designated bridge is located between the local switch and the root bridge.

Desig. Cost
The sum of all the root port costs on all bridges, including the switch, between the switch and the root bridge.

Desig. Bridge
An adjacent bridge to which the root port of the switch is actively connected.

Desig. Port
The port on the designated bridge that is directly connected to the root port of the local switch.

Chapter 10

802.1x Port-based Network Access Control

This chapter contains information about and the procedure for configuring 802.1x Port-based Network Access Control. It includes the following sections:

802.1x Port-based Network Access Control Overview

802.1x Port-based Network Access Control (IEEE 802.1x) is used to control who can send traffic through and receive traffic from a switch port. With this feature, the switch will not allow an end node to send or receive traffic through a port until the user of the node logs on by entering a username and password.

This feature can prevent an unauthorized individual from connecting a computer to a switch port or using an unattended workstation to access your network resources. Only those users to whom you have assigned a username and password will be able to use the switch to access the network.

This feature must be used with the RADIUS authentication protocol and requires that there be a RADIUS server on your network. The RADIUS server performs the authentication of the username and password combinations.

Note
RADIUS with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server for this feature.

Following are several terms to keep in mind when using this feature.

- Supplicant - A supplicant is an end user or end node that wants to access the network through a switch port. A supplicant is also referred to as a client.
- Authenticator - The authenticator is a port on the switch that prohibits network access by a supplicant until the network user has entered a valid username and password.
- Authentication server - The authentication server is the network device that has the RADIUS server software. This is the device that does the actual authenticating of the user names and passwords from the supplicants.

The AT-GS950/16 and AT-GS950/24 switches do not authenticate the usernames and passwords from the end users. Rather, they act as an intermediary between a supplicant and the authentication server during the authentication process.

Authentication Process

Below is a brief overview of the authentication process that occurs between a supplicant, authenticator, and authentication server. For further details, refer to the IEEE 802.1x standard.

- Either the authenticator (that is, a switch port) or the supplicant can initiate an authentication prompt exchange. The switch initiates an exchange when it detects a change in the status of a port (such as when the port transitions from no link to valid link), or if it receives a packet on the port with a source MAC address not in the MAC address table.
- An authenticator starts the exchange by sending an EAP-Request/Identity packet. A supplicant starts the exchange with an EAPOL-Start packet, to which the authenticator responds with a EAP-Request/Identity packet.
- The supplicant responds with an EAP-Response/Identity packet to the authentication server via the authenticator.
- The authentication server responds with an EAP-Request packet to the supplicant via the authenticator.
- The supplicant responds with an EAP-Response/MDS packet containing a username and password.
- The authentication server sends either an EAP-Success packet or EAP-Reject packet to the supplicant.
- Upon successful authorization of the supplicant by the authentication server, the switch adds the supplicant's MAC address to the MAC address as an authorized address and begins forwarding network traffic to and from the port.
- When the supplicant sends an EAPOL-Logoff prompt, the switch removes the supplicant's MAC address from the MAC address table, preventing the supplicant from sending or receiving any further traffic from the port.

Authenticator Ports

All of the ports on the AT-9400 Series switch are authenticator ports. An authenticator port can have one of three settings. These settings are referred to as the port control settings. The settings are:

- Auto - Activates 802.1x port-based authentication. An authenticator port with this setting does not forward network traffic to or from the end node until the client has entered a username and password that the authentication server must validate. The port begins in the unauthorized state, sending and receiving only EAPOL frames. All other frames, including multicast and broadcast frames, are discarded. The authentication process begins when the link state of the port changes or the port receives an EAPOL-Start packet from a supplicant. The switch requests the identity of the client and begins relaying authentication prompts between the client and the authentication server. Each client that attempts to access the network is uniquely identified by the switch using the client's MAC address.

- Force-unauthorized - Places the port in the unauthorized state, ignoring all attempts by the client to authenticate. This port control setting blocks all users from accessing the network through the port and is similar to disabling a port and can be used to secure a port from use. The port continues to forward EAPOL packets, but discards all other packets, including multicast and broadcast packets.
- Force-authorized - Disables IEEE 802.1x port-based authentication and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1x-based authentication of the client. This is the default setting. Use this port control setting for those ports where there are network devices that are not to be authenticated.

Figure 34 illustrates the concept of the authenticator port control settings.

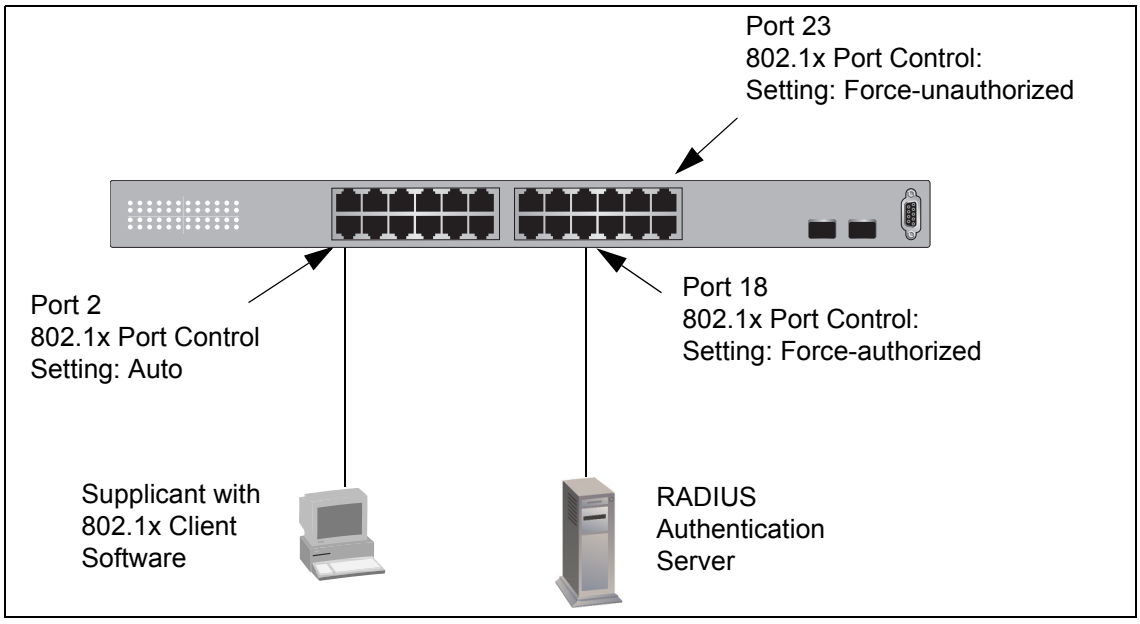


Figure 34. Example of the Authenticator Role

- Port 2 is set to Auto. The end node connected to the port must use its 802.1x client software and provide a username and password to send or receive traffic from the switch.
- Port 18 is set to the Force-authorized setting so that the end node connected to the port does not have to provide a user name or password to send or receive traffic from the switch. In the example, the node is the RADIUS authentication server. Since the server cannot authenticate itself, its port must be set to Force-authorized in order for it to pass traffic through the port.
- Port 23 is set to Force-unauthorized to prevent anyone for using the port.

As mentioned earlier, the switch itself does not authenticate the user names and passwords from the clients. That is the responsibility of the authentication server, which contains the RADIUS server software. Instead, a switch acts as an intermediary for the authentication server by denying access to the network by the client until the client has provided a valid username and password, which the authentication server validates.

General Steps

Following are the general steps to implementing 802.1x Port-based Network Access Control:

1. You must install RADIUS server software on one or more of your network servers or management stations. Authentication protocol server software is not available from Allied Telesyn. Funk Software Steel-Belted Radius and Free Radius have been verified as fully compatible with the AT-S79 management software.

2. You need to install 802.1x client software on those workstations that are to be supplicants. Microsoft WinXP client software and Meeting House Aegis client software have been verified as fully compatible with the AT-S79 management software.

3. You must configure and activate the RADIUS client software in the AT-S79 management software. The default setting for the authentication protocol is disabled. You will need to provide the following information:

   - The IP address of a RADIUS servers.
   - The encryption key used by the authentication server.

   For instructions, refer to Chapter 11, "RADIUS Authentication Protocol" on page 141.

4. You must configure the authenticator port settings, as explained in "Configuring 802.1x Port-based Network Access Control" on page 136 in this chapter.

Port-based Network Access Control Guidelines

Following are the guidelines for using this feature:

- Ports set to Auto do not support port trunking or dynamic MAC address learning.
- The appropriate setting for a port on an AT-GS950/16 or AT-GS950/24 switch connected to an authentication server is Force-authorized, the default setting. This is because an authentication server cannot authenticate itself.
- The authentication server must be a member of the Default VLAN by communicating with the switch through a port that is an untagged member of the Default VLAN.

- Allied Telesyn does not support connecting more than one supplicant to an authenticator port on the switch. The switch allows only one supplicant to log on per port.

  Note
  Connecting multiple supplicants to a switch port set to the Auto setting does not conform to the IEEE 802.1x standard. This can introduce security risks and can result in undesirable switch behavior. To avoid this, Allied Telesyn recommends use the Force-authorized setting on those ports that are connected to more than one end node, such as a port connected to another switch or to a hub.

- A username and password combination is not tied to the MAC address of an end node. This allows end users to use the same username and password when working at different workstations.
- After a supplicant has successfully logged on, the MAC address of the end node is added to the switch's MAC address table as an authenticated address. It remains in the table until the end user logs off the network. The address is not timed out, even if the end node becomes inactive.

  Note
  End users of port-based access control should be instructed to always log off when they are finished with a work session. This prevents unauthorized individuals from accessing the network through unattended network workstations.

- There should be only one port in the authenticator port control setting of Auto between a client and the authentication server.

- Ports used to interconnect switches should be set to the port control setting of Force-authorized. This is illustrated in Figure 35.

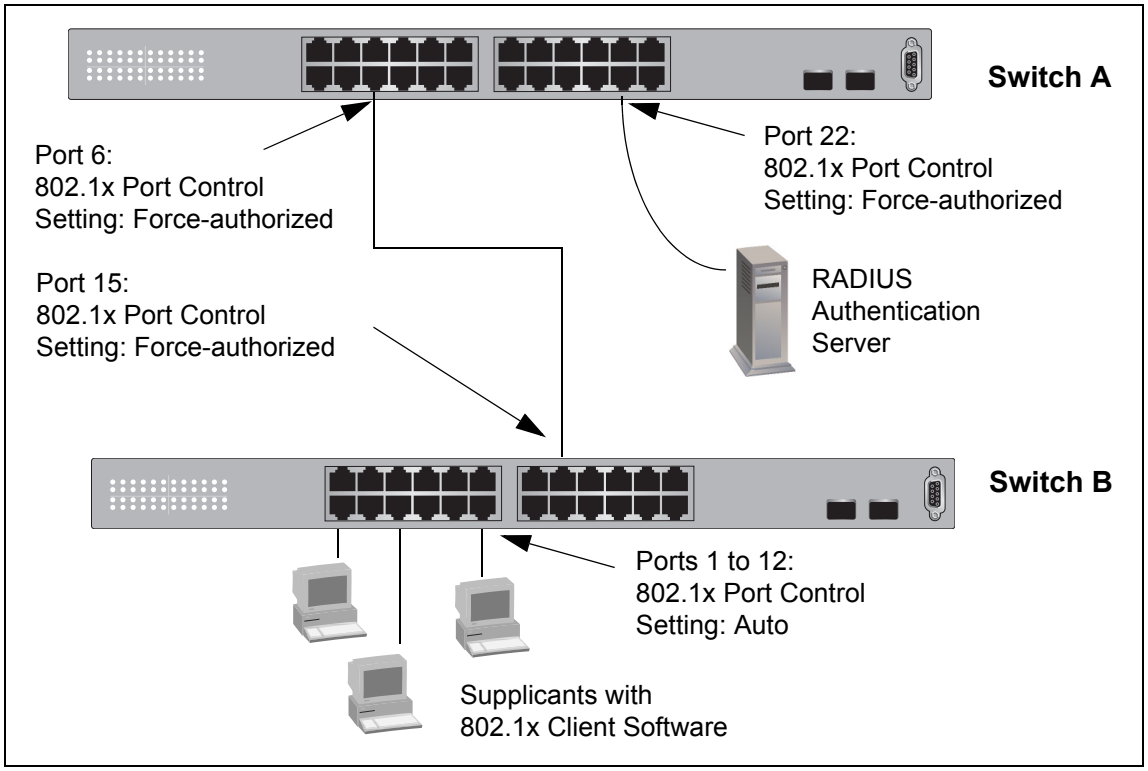


Figure 35. Port-based Authentication Across Multiple Switches

Configuring 802.1x Port-based Network Access Control

To configure 802.1x port-based network access control, perform the following procedure:

1. From the Main Menu, type **A** to select **Advanced Switch Configuration**.

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 59.

2. From the Advanced Switch Configuration Menu, type **X** to select **802.1x Port Based Access Control Configuration**.

   The Port Based Access Control Configuration Menu is shown in Figure 36.

```
AT-GS950/16 Local Management System
Advanced Switch Configuration -> Port Based Access Control Configuration Menu

NAS ID                    : Nas1
Port No                   : 1
Port Status               : Authorized
Port Control              : Force Authorized
Transmission Period       : 30    seconds
Supplicant Timeout        : 30    seconds
Server Timeout            : 30    seconds
Maximum Request           : 2
Quiet Period              : 60    seconds
Re-authentication Period  : 3600  seconds
Re-authentication Status  : Disabled


---------------------- <COMMAND> -----------------------------------
[N]AS ID                    Server Time[o]ut        [I]nitialize
[P]ort No                   [M]aximum Request       [R]e-auth Initialize
Port [C]ontrol              Q[u]iet Period          [Q]uit to previous Page
[T]ransmission Period       R[e]-auth Period
Supp[l]icant Timeout        Re-[a]uth Status



Command>
```

Figure 36. Port Based Access Control Configuration Menu

3. Type **P** to select **Port No**.

   The following prompt is displayed:

   ```
   Enter port number>
   ```

4. Enter the number of the port on the switch you want to configure. You can configure only one port at a time.

   The Port Based Access Control Configuration Menu is updated with the current settings of the selected port.

5. Configure the 802.1x settings for the port. A change to a parameter takes affect immediately on the port. The settings are described here:

   NAS ID.
   This parameter assigns an 802.1x identifier to the switch that applies to all ports. The NAS ID can be up to sixteen characters. Valid characters are 0 to 9, a to z, and A to Z. Spaces are allowed. Specifying an NAS ID is optional.

   Port Status.
   Displays the current 802.1 status of the port as either authorized or unauthorized. This is not an adjustable parameter.

   Port Control.
   Sets the 802.1x port control setting. The possible settings are:

   A (Auto) - Enables 802.1x port-based authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes or the port receives an EAPOL-Start packet from a supplicant. The switch requests the identity of the client and begins relaying authentication prompts between the client and the authentication server.

   U (Force-unauthorized) **-** Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate.

   F (Force-authorized) - Disables IEEE 802.1x port-based authentication and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1x-based authentication of the client. This is the default setting.

   Transmission Period.
   Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The default value is 30 seconds. The range is 1 to 65,535 seconds.

Supplicant Timeout.
Sets the switch-to-client retransmission time for the EAP-request frame. The default value for this parameter is 30 seconds. The range is 1 to 600 seconds.

Server Timeout.
Sets the timer used by the switch to determine authentication server timeout conditions. The default value for this parameter is 10 seconds. The range is 1 to 60 seconds.

Maximum Request.
Sets the maximum number of times that the switch retransmits an EAP Request packet to the client before it times out the authentication session. The default value for this parameter is 2 retransmissions. The range is 1 to 10 retransmissions.

Quiet Period.
Sets the number of seconds that the port remains in the quiet state following a failed authentication exchange with the client. The default value is 60 seconds. The range is 0 to 65,535 seconds.

Re-auth Period.
Specifies the time period between periodic reauthentication of the client. The default value is 3600 seconds. The range is 1 to 65,535 seconds.

Re-auth Status.
Specifies if reauthentication should occur according to the reauthentication period. The options are Enabled or Disabled.

6. If the port control setting is Auto and you want to return the EAPOL machine state on the port to the initialized state, do the following:

   a. Type **I** to select **Initialize**.

      The following prompt is displayed:

      ```
      Would you initialize authenticator? (Y/N)>
      ```

   b. Typing **Y** returns the EAPOL machine state on the port to the initialize state. Typing **N** cancels the step.

7. If the port control setting is Auto and you want the node connected to the port to reauthenticate with the RADIUS server, do the following:

   a. Type **R** to select **Re-auth Initialize**.

      The following prompt is displayed:

      ```
      Initialize re-authentication? (Y/N)>
      ```

b. Typing **Y** returns the port to the unauthenticated state and the re-authentication period to zero. The user must enter a valid username and password to continue to use the switch port. Typing **N** cancels the reauthentication.

8. Type **Q** to select **Quit to previous menu** and save the settings.

Chapter 11

RADIUS Authentication Protocol

This chapter describes how to configure the RADIUS client software on the switch. You can use the RADIUS client with 802.1x port-based network access control to control who can forward packets through the switch. Sections in the chapter include:

RADIUS Overview

RADIUS (Remote Authentication Dial In User Services) is an authentication protocol for enhancing the security of your network. The protocol transfers the task of authenticating network access from a network device to an authentication protocol server.

The AT-S79 management software comes with RADIUS client software. You can use the client software together with 802.1x port-based network access control, described in Chapter 10, “802.1x Port-based Network Access Control” on page 129, to control which end users and end nodes can send packets through the switch.

RADIUS Implementation Guidelines

What do you need to use the RADIUS protocol? Following are the main points.

- You must install RADIUS server software on a network server or management station. Authentication protocol server software is not available from Allied Telesyn.
- The RADIUS server must be communicating with the switch through a port that is an untagged member of the Default VLAN.
- If the RADIUS server is on a different subnet from switch, be sure to specify a default gateway in the System IP Configuration Menu, shown in Figure 5 on page 31, so that the switch and server can communicate with each other.
- You need to configure the RADIUS server software on the authentication server by specifying the username and password combinations. The maximum length of a username or password is 12 alphanumeric characters.

  Note
  This manual does not explain how to configure RADIUS server software. Refer to the documentation that came with the software for instructions.

- You must activate the RADIUS client software on the switch using the AT-S79 management software and configure the settings. This is explained in “Configuring the RADIUS Client” on page 143. By default, authentication protocol is disabled.

  Note
  For more information on the RADIUS authentication protocol, refer to the RFC 2865 standard.

Configuring the RADIUS Client

To configure the RADIUS client, perform the following procedure:

1. From the Main Menu, type **B** to select **Basic Switch Configuration**.

   The Basic Switch Configuration Menu is shown in Figure 4 on page 30.

2. From the Basic Switch Configuration Menu, type **U** to select **User Interface Configuration**.

   The User Interface Configuration Menu is shown in Figure 7 on page 36.

3. Type **R** to select **RADIUS Server Configuration**.

   The RADIUS Server Configuration Menu is shown in Figure 37.

```
AT-GS950/16 Local Management System
Basic Switch Configuration -> RADIUS Server Configuration Menu

Server IP Address      :  0.0.0.0
Shared Se[c]ret        :
Response Time          :  10 seconds
Maximum Retransmission :  3

---------------------- <COMMAND> -----------------------------
Set Server [I]P
Set Shared Se[c]ret
Set [R]esponse Time
Set [M]ax Retransmission
[Q]uit to previous menu


Command>
```

Figure 37. RADIUS Server Configuration Menu

4. Type **I** to select **Set Server IP**.

   The following prompt is displayed:

   ```
   Enter IP address for RADIUS server>
   ```

5. Type the IP address of the RADIUS server and press Enter.

6. Type **C** to select **Shared Secret**.

   The following prompt is displayed:

   ```
   Enter secret string for server>
   ```

7. Enter the encryption key of the RADIUS server.
8. Type **R** to select **Set Response Time**.

   The following prompt is displayed:

   ```
   Enter response time>
   ```

9. Enter the amount of time in seconds the switch should wait for a response from the RADIUS server. The range is 1 to 120 seconds. The default is 10 seconds.
10. Type **M** to select **Max Retransmission**.

    The following prompt is displayed:

    ```
    Enter maximum retransmissions>
    ```

11. Enter the number of times the switch should retransmit to the RADIUS server in the event the server does not respond. The range is 1 to 254. The default is 3.
12. Type **Q** to select **Quit to previous menu** and save your changes.

Displaying the RADIUS Client Settings

To display the RADIUS client status and settings, perform the following procedure:

1. From the Main Menu, type **B** to select **Basic Switch Configuration**.

   The Basic Switch Configuration Menu is shown in Figure 4 on page 30.

2. From the Basic Switch Configuration Menu, type **U** to select **User Interface Configuration**.

   The User Interface Configuration Menu is shown in Figure 7 on page 36.

3. Type **R** to select **RADIUS Server Configuration**.

   The RADIUS Server Configuration Menu is shown in Figure 37 on page 143. The top of the menu shows the current RADIUS server configuration.

4. Type **Q** to return to the previous menu.

Chapter 12

Broadcast Storm Control

This chapter describes how to configure the broadcast storm control feature on the switch and includes the following sections:

Broadcast Storm Control Overview

The broadcast storm control feature limits the number of broadcast frames forwarded by the switch. The feature can help improve network performance in situations where broadcast frames are consuming a significant portion of network bandwidth, to a degree where the remaining bandwidth is insufficient for efficiently carrying the unicast and multicast frames.

This feature can also protect your network from broadcast storms. Broadcast storms commonly occur when an Ethernet network topology contains a loop and where the Spanning Tree Protocol is not implemented. Ethernet frames become caught in repeating cycles that needlessly consume network bandwidth.

The default setting for this feature is disabled. In the default setting, the switch forwards all ingress broadcast frames, provided that ports are not over-subscribed.

When you enable the feature, you are given three threshold levels from which to choose. The levels prescribe the maximum number of ingress broadcast frames the switch will accept per second. Broadcast frames that exceed the limit are discarded. The level are:

- ❒ High: 3000 broadcast packets per second
- ❒ Medium: 500 broadcast packets per second
- ❒ Low: 100 broadcast packets per second

For example, activating the feature and selecting Medium as the threshold means that the switch accepts up to a maximum of 500 ingress broadcast packets per second and discards those broadcast packets that exceed the limit.

Configuring Broadcast Storm Control

To configure the broadcast storm control feature, perform the following procedure:

1. From the Main Menu, type **B** to select **Basic Switch Configuration**.

   The Basic Switch Configuration Menu is shown in Figure 4 on page 30.

2. From the Basic Switch Configuration Menu, type **C** to select **Storm Control Configuration**.

   The Storm Control Configuration Menu is shown in Figure 38.

```
AT-GS950/16 Local Management System
Basic Switch Configuration -> Storm Control Configuration Menu

Broadcast Storm Status :  Disabled

Threshold :  Low

---------------------- <COMMAND> -----------------------------
Set [B]roadcast Status
Set [T]hreshold
[Q]uit to previous menu


Command>
```

Figure 38. Storm Control Configuration Menu

3. Type **B** to select **Broadcast Storm Status**.

   The following prompt is displayed:

   ```
   Enable or Disable broadcast storm control (E/D)>
   ```

4. Type **E** to enable broadcast storm control or **D** to disable broadcast storm control.

5. If you are activating the feature, type **T** to select Threshold.

   The following prompt is displayed:

   ```
   Enter threshold level>
   ```

6. Specify the broadcast threshold. Choices are:

   - **H** for High (3000 broadcast packets per second)
   - **M** for Medium (500 broadcast packets per second)

- **L** for Low (100 broadcast packets per second)

7. Type **Q** to quit to the previous menu and save your changes.

Chapter 13

Management Software Updates

The procedure in this chapter explains how to download a new version of the AT-S79 management software onto the switch. The procedure is:

- “Downloading a New Management Software Image Using TFTP” on page 152

Note
For information on how to obtain new releases of the AT-S79 management software, refer to “Management Software Updates” on page 14.

Downloading a New Management Software Image Using TFTP

Before downloading a new version of the AT-S79 management software onto the switch, note the following:

- Both models of the AT-GS950 series use the same AT-S79 management software image.
- The current configuration of a switch is retained when a new AT-S79 software image is installed. To return a switch to its default configuration values, refer to “Returning the AT-S79 Management Software to the Factory Default Values” on page 47.
- Your network must have a node with TFTP server software.
- You must store the new AT-S79 image file on the server.
- You should start the TFTP server software before you begin the download procedure.
- The switch where you are downloading the new image file must have an IP address and subnet mask. For instructions on how to configure the IP address on a switch, refer to “Configuring the IP Address, Subnet Mask, and Gateway Address” on page 30 or “Enabling and Disabling the DHCP Client” on page 33.

Caution

Downloading a new version of management software onto the switch causes the device to reset. Some network traffic may be lost during the reset process.

The following procedure assumes you have already obtained the new software from Allied Telesyn and stored it on the TFTP server.

To download the AT-S79 image software onto the switch, perform the following procedure:

1. From the Main Menu, type **T** to select **Switch Tools**.

   The Switch Tools Configuration Menu is shown in Figure 9 on page 42.

2. From the Switch Tools Menu, type **U** to select **Software Upgrade**.

The Software Upgrade Menu is shown in Figure 39.

```
AT-GS950/16 Local Management System
Switch Tools Configuration -> Software Upgrade Menu

[T]FTP Software Upgrade
[Q]uit to previous menu




Command>
```

Figure 39. Software Upgrade Menu (1 of 2)

3. Type **T** to select **TFTP Upgrade**.

   The Software Upgrade Menu (2 of 2) is shown in Figure 40.

```
AT-GS950/16 Local Management System
Main Menu -> Software Upgrade Menu

Image Version/Date:   0.0.0L/Jul 29 2006 20:57:07

TFTP Server IP:       0.0.0.0
Image File Name:
Retry Count:          5

---------------------- <COMMAND> -------------------------

Set TFTP [S]erver IP Address
Set Image [F]ile Name
[U]pgrade Image and Reboot
Set [R]etry Count
[Q]uit to previous menu




Command>
```

Figure 40. Software Upgrade Menu (2 of 2)

4. Type **S** to select **Set TFTP Server IP Address**.

   The following prompt is displayed:

   ```
   Enter IP address of TFTP server:
   ```

5. Type the IP address of the TFTP server and press Enter.

6. Type **F** to select **Set Image File Name**.

   The following prompt is displayed:

   ```
   Enter file name>
   ```

7. Enter the file name of the AT-S79 image file on the TFTP server and press Enter.

8. Type **R** to select **Set Retry Count**.

   The following prompt is displayed:

   ```
   Enter retry count>
   ```

9. Enter the number of times you want the switch to retry in the event a problem occurs during the download process. The range is 1 to 20. The default is 5 times.

10. To begin the download, type **U** to select **Upgrade Image and Reboot**.

    The following prompt is displayed:

    ```
    Download file? (Y/N)>
    ```

11. Type **Y** for yes to begin the upgrade or **N** for no to cancel the procedure.

    If you select yes, the software immediately begins to download the file onto the switch. After the software download is complete, the switch initializes the software and reboots. You will lose your local management connection to the switch during the reboot process.

Section II

Using the Web Browser Interface

The chapters in this section provide information and procedures for using the web browser interface in the AT-S79 management software. The chapters include:

Chapter 14

Starting a Web Browser Management Session

This chapter contains the procedures for starting, using, and quitting a web browser management session on the AT-GS950/16 and AT-GS950/24 Smart Switches. Sections in the chapter include:

Establishing a Remote Connection to Use the Web Browser Interface

In order for you to manage an AT-GS950/16 or AT-GS950/24 Smart Switch using the web browser interface, the switch must have an IP address and subnet mask. To manually assign an IP address, refer to “Configuring the IP Address, Subnet Mask, and Gateway Address” on page 30. To configure the switch to obtain its IP configuration from a DHCP server, refer to “Enabling and Disabling the DHCP Client” on page 33. The initial assignment of an IP address must be made through a local management session.

Note
Enhanced stacking, a feature of other Allied Telesyn Layer 2 and Layer 2+ managed switches, is not supported by the AT-GS950/16 and AT-GS950/24 Smart Switches.

Note
The remote management station must be a member of the switch’s Default VLAN. The switch responds and processes management packets only if they are received on an untagged port of the Default VLAN.

To start a web browser management session, perform the following procedure:

1. Start your web browser.

   Note
   If your PC with the web browser is connected directly to the switch to be managed or is on the same side of a firewall as the switch, you must configure your browser’s network options not to use proxies. Consult your web browser’s documentation on how to configure the switch’s web browser to not use proxies.

2. In the URL field of the browser, enter the IP address of the switch to be managed.

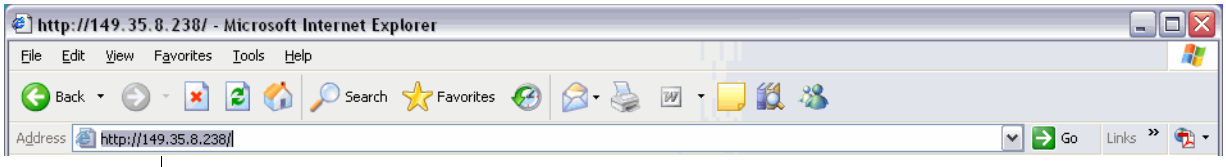


Figure 41. Entering a Switch’s IP Address in the URL Field

The AT-S79 management software displays the login dialog box, shown in Figure 42.

Figure 42. AT-S79 Login Dialog Box

3. Enter the AT-S79 management login user name and password. The default user name and password are both "manager". The login name and password are case-sensitive.

   To change the user name and password, refer to "Configuring System Administration Information" on page 167.

   The AT-S79 management software displays the home page. The window contains an image of the front of the switch. Ports that have a link to an end node are green. Ports without a link are grey. An example of a home page is shown in Figure 43.

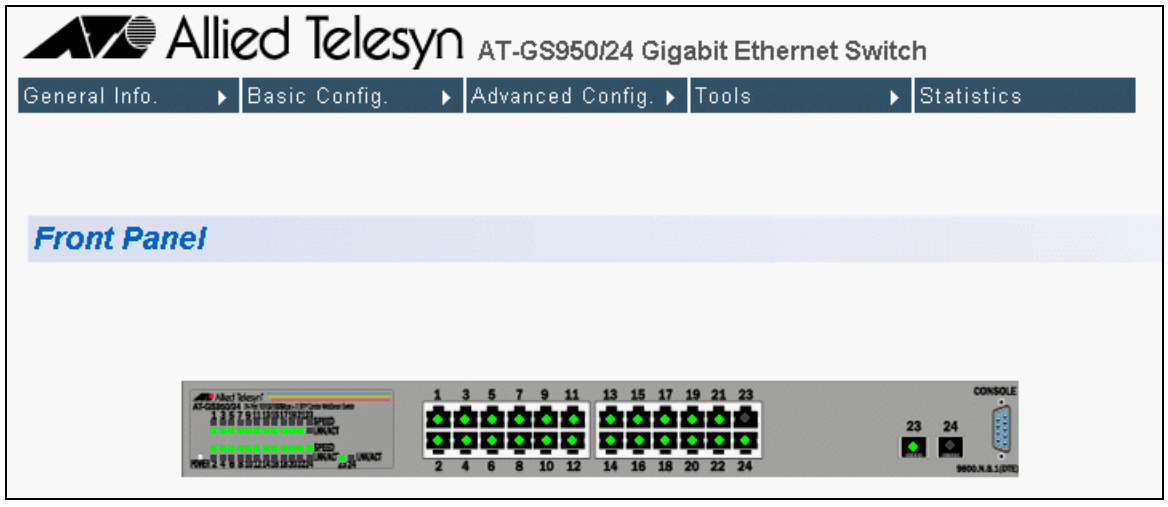


Figure 43. Home Page for the AT-GS950/24

The main menu is on the top of the home page. It consists of the following selections:

- General Info.
- Basic Config.
- Advanced Config.
- Tools
- Statistics

A web browser management session remains active even if you link to other sites. You can return to the management web pages anytime as long as you do not quit the browser.

Web Browser Tools

You can use the web browser tools to move around the management pages. Selecting **Back** on your browser's toolbar returns you to the previous display. You can also use the browser's **bookmark** feature to save the link to the switch.

Quitting a Web Browser Management Session

To exit a web browser management session, close the web browser.

Chapter 15

Basic Switch Parameters

This chapter contains the following sections:

Configuring an IP Address, Subnet Mask and Gateway Address

This procedure explains how to change the IP address, subnet mask, and gateway address to the switch. Before performing the procedure, note the following:

- An IP address and subnet mask are not required for normal network operations of the switch. Values for these parameters are only required if you want to remotely manage the device with a web browser.
- A gateway address is only required if you want to remotely manage the device from a remote management station that is separated from the switch by a router.
- To configure the switch to automatically obtain its IP configuration from a DHCP server on your network, go to “Enabling and Disabling the DHCP Client” on page 166.
- The initial assignment of an IP address must be made through a local management session using the menus interface.

To change the switch’s IP configuration, perform the following procedure:

1. From the **Basic Config** menu, select **IP Config**.

   The IP Configuration page is shown in Figure 44.

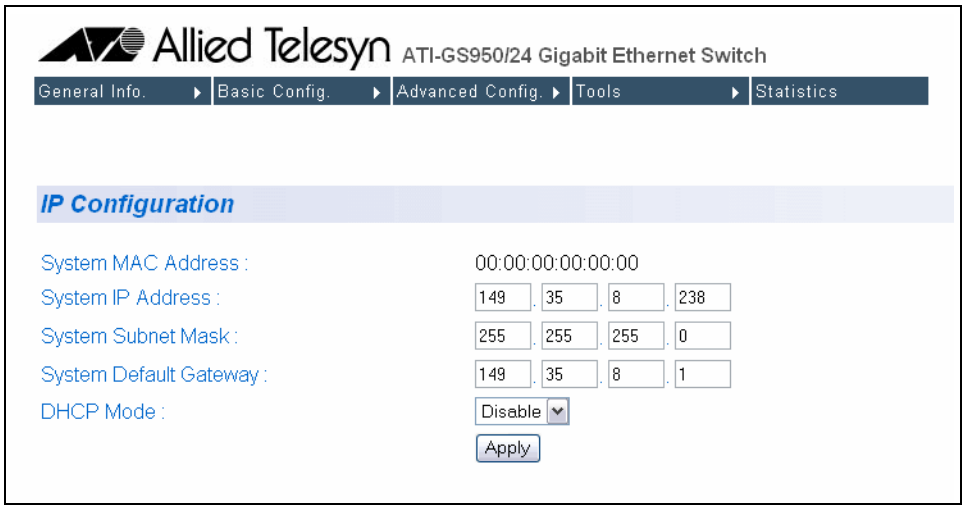


Figure 44. IP Configuration Page

2. Change the IP configuration parameters by entering new information in the fields:

   System MAC Address
   This parameter displays the MAC address of the switch. You cannot change this parameter.

System IP Address
Enter the IP address for the switch.

System Subnet Mask
Enter the subnet mask for the switch.

System Default Gateway
Enter the default gateway's IP address.

DHCP Mode
For information about setting this parameter, refer to "Enabling and Disabling the DHCP Client" on page 166.

3. Click **Apply**.

Note
Changing the IP address ends your management session. To resume managing the device, enter the new IP address of the switch in the web browser's URL field, as shown in Figure 41 on page 158.

Enabling and Disabling the DHCP Client

This procedure explains how to activate and deactivate the DHCP client on the switch. When the client is activated, the switch obtains its IP configuration, such as its IP address and subnet mask, from a DHCP server on your network. Before performing the procedure, note the following:

- An IP address and subnet mask are not required for normal network operations of the switch. Values for these parameters are only required if you want to remotely manage the device with a web browser.
- A gateway address is only required if you want to remotely manage the device from a remote management station that is separated from the switch by a router.
- The DHCP client is disabled by default on the switch.
- The DHCP client does not support BOOTP.
- The initial assignment of the IP address must be made through a local management session using the menus interface.

To activate or deactivate the DHCP client on the switch, perform the following procedure:

1. From the **Basic Config** menu, select **IP Config**.

   The IP Configuration page is shown in Figure 44 on page 164.

2. For the **DHCP Mode**, select **Enable** or **Disable**.

3. Click **Apply**.

   If you enable the client, it immediately begins to send queries to the DHCP server. It continues to send queries until it receives a response.

Note
Enabling DHCP ends your management session. To resume managing the device, enter the IP address assigned to the switch by the DHCP server in the web browser's URL field.

Configuring System Administration Information

This section explains how to assign a name to the switch, as well as the location of the switch and the name of the switch's administrator. Entering this information is optional.

To set a switch's administration information, perform the following procedure:

1. From the **Basic Config** menu, select **Admin. Config**.

   The Administration Configuration page is shown in Figure 45.

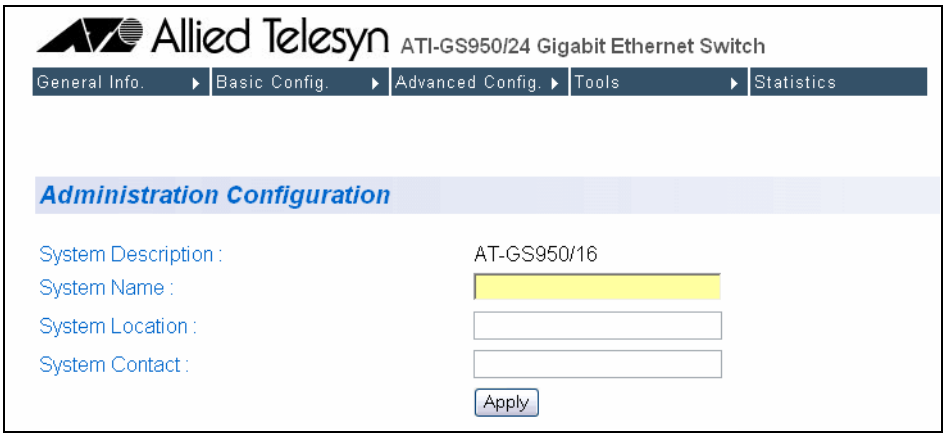


Figure 45. Administration Configuration Page

2. Configure the following parameters as necessary:

   System Description
   Specifies the model number of the switch. You cannot change this parameter.

   System Name
   Specifies a name for the switch, for example, Sales. The name is optional and may contain up to 50 characters.

   Note
   Allied Telesyn recommends that you assign a name to the switch. A name can help you identify the switch when you manage it and can also help you avoid performing a configuration procedure on the wrong switch.

   System Location
   Specifies the location of the switch. The location is optional and may contain up to 50 characters.

System Contact
Specifies the name of the network administrator responsible for managing the switch. This contact name is optional and may contain up to 50 characters.

3. Click **Apply**.

Setting the User Interface Configuration

This procedure explains how to adjust the user interface and security features on the switch. With this procedure you can:

- Change the console timer, used to automatically end inactive local management sessions.
- Change the AT-S79 management login user name and password.
- Enable and disable the web server, used to manage the switch from a remote management station with a web browser.

To set the switch's user interface configuration, perform the following procedure:

1. From the **Basic Config** menu, select **User Interface**.

   The User Interface page is shown in Figure 46.

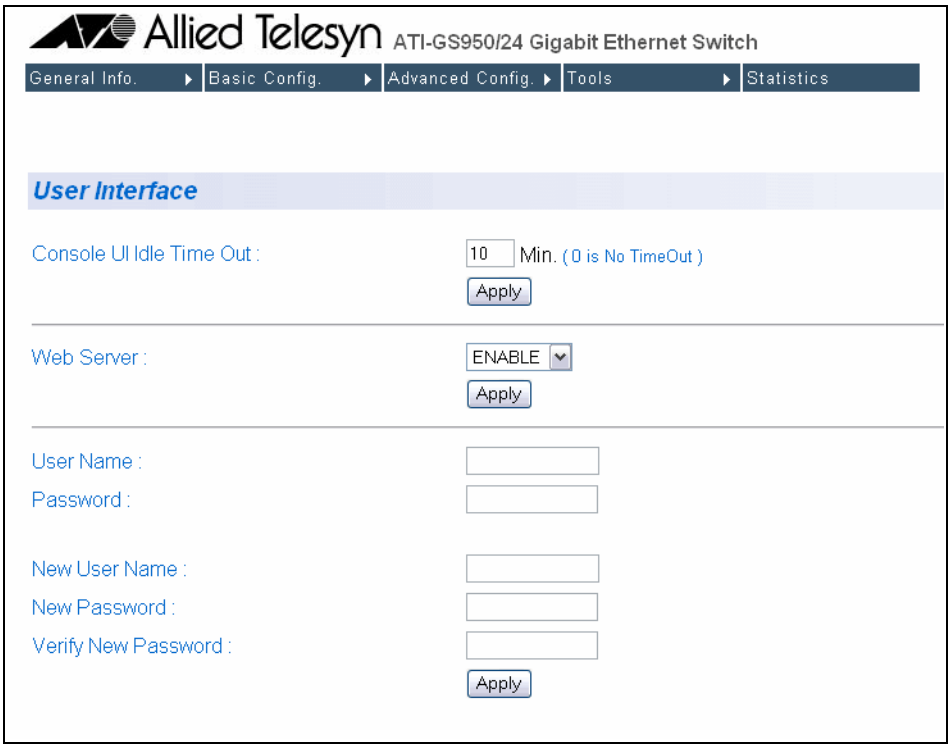


Figure 46. User Interface Page

The User Interface page has three parts:

- Console UI Idle Time Out
- Web Server
- User name and password

2. To configure the console idle time out parameter, do the following:

   a. Click the **Console UI Time Out** field and enter a new value. The range is 0 to 60 minutes. The default is 5 minutes. A timeout value to 0 causes the console connection to never times out.

      The console idle time out parameter specifies the length of time a local management session can be inactive before the management software automatically ends it. The purpose of this parameter is to prevent unauthorized individuals from configuring the switch should you leave your management workstation unattended.

      This parameter applies to a local management session but not to a web management session. A web browser management session remains active so long as your web browser is open.

      Note
      If you select 0, you must remember to properly log off from a local management session when you are finished to prevent blocking future management sessions with the switch.

   b. Click **Apply**.

3. To enable or disable the web server, do the following:

   a. Click the **Web Server** parameter and choose **Enable** or **Disable** from the list. The default is Enable. When you enable this parameter, an individual can manage the switch remotely using a web browser.

      Note
      Disabling the web browser automatically ends your remote management session.

   b. Click **Apply**.

4. To change the AT-S79 management login name or password, do the following:

   a. Enter the existing name and password in the **User Name** and **Password** fields. The default name and password are both “manager”. The login name and password are case sensitive.

   b. Click the **New User Name** field and enter a new user name or, if you do not want to change the login name, enter the current name. Leaving this field empty deletes the current login name without assigning a new one. The name can be from 0 to 12 characters. Spaces are allowed. The login name is case sensitive.

c. Click the **New Password** field and enter a new login password or, if you do not want to change the password, enter the current password. The password can be from 0 to 12 characters. Allied Telesyn recommends not using special characters, such as spaces and exclamation points. The password is case sensitive. Leaving this field empty deletes the current password without assigning a new one.

d. Click the **Verify New Password** field and enter the same password entered in the previous step.

e. Click **Apply**.

Viewing System Information

To view general information about the switch, perform the following procedure:

1. From **General Info.** menu, select **Switch Information**.

   The Switch Information page is shown in Figure 47.

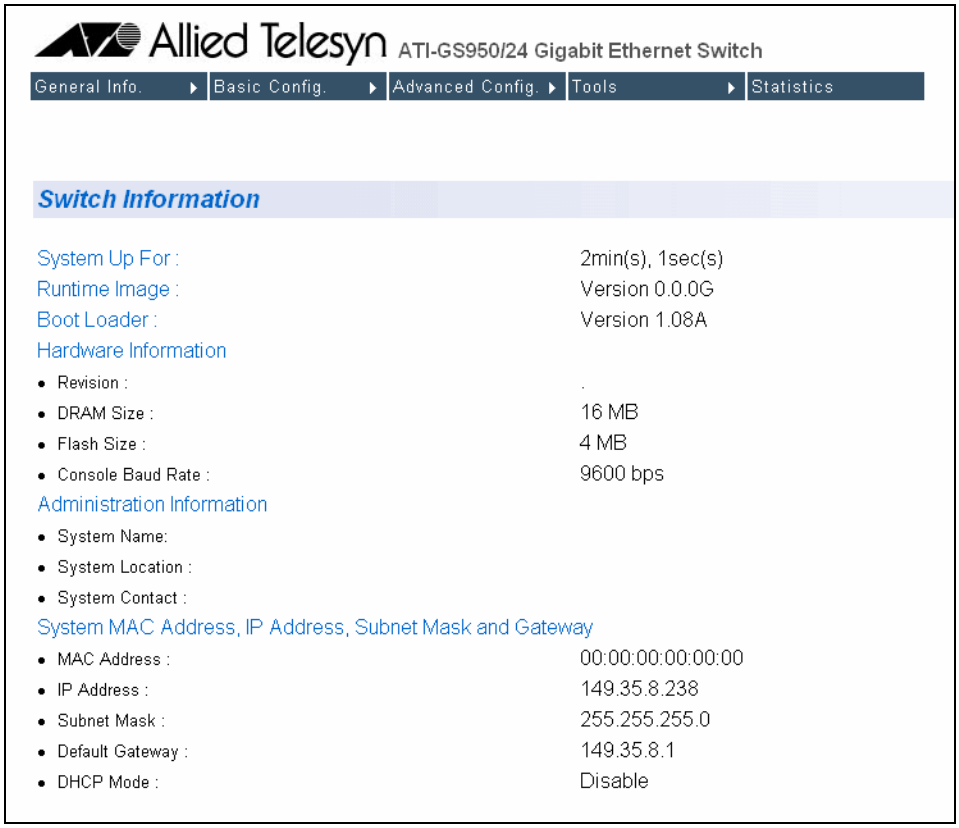


Figure 47. Switch Information Page

The Switch Information page displays the following information:

System Up Time
The number of days, hours, and minutes that the switch has been running since it was last rebooted.

Runtime Image
The version number and build date of the runtime firmware.

Boot Loader
The version number and build date of the bootloader firmware.

Hardware Information Section:

Reversion
The hardware version number.

DRAM Size
The size of the DRAM, in megabytes.

Flash Size
The size of the flash memory, in megabytes.

Fixed Baud Rate
The baud rate of the console port.

Administration Information Section:

Switch Name
The name assigned to the switch. To give the switch a name, refer to "Configuring System Administration Information" on page 167.

Switch Location
The location of the switch. To specify the location, refer to "Configuring System Administration Information" on page 167.

Switch Contact
The contact person responsible for managing the switch. To specify the name of a contact, refer to "Configuring System Administration Information" on page 167.

System MAC Address, IP Address, Subnet Mask, and Gateway Section:

MAC Address
The MAC address of the switch. You cannot change this value.

IP Address
The IP address of the switch. Refer to "Configuring an IP Address, Subnet Mask and Gateway Address" on page 164 to manually assign an IP address or "Enabling and Disabling the DHCP Client" on page 166 to activate the DHCP client.

Subnet Mask
The subnet mask for the switch. Refer to "Configuring an IP Address, Subnet Mask and Gateway Address" on page 164 to manually assign a subnet mask or "Enabling and Disabling the DHCP Client" on page 166 to activate the DHCP client.

Default Gateway
Default gateway's IP address. Refer to "Configuring an IP Address, Subnet Mask and Gateway Address" on page 164 to manually assign a gateway address or "Enabling and Disabling the DHCP Client" on page 166 to activate the DHCP client.

DHCP Mode
The status of the DHCP client on the switch. For information about setting this parameter, refer to “Enabling and Disabling the DHCP Client” on page 166.

Rebooting a Switch

This procedure reboots the switch and reloads the AT-S79 management software from flash memory. You might reboot the device if you believe it is experiencing a problem. Rebooting the device does not change any of the device's parameter settings.

Caution
The switch does not forward network traffic during the reboot process. Some network traffic may be lost.

To reboot a switch, perform the following procedure:

1. From the **Tools** menu, select **System Reboot**.

   The System Reboot Configuration page is shown in Figure 48.

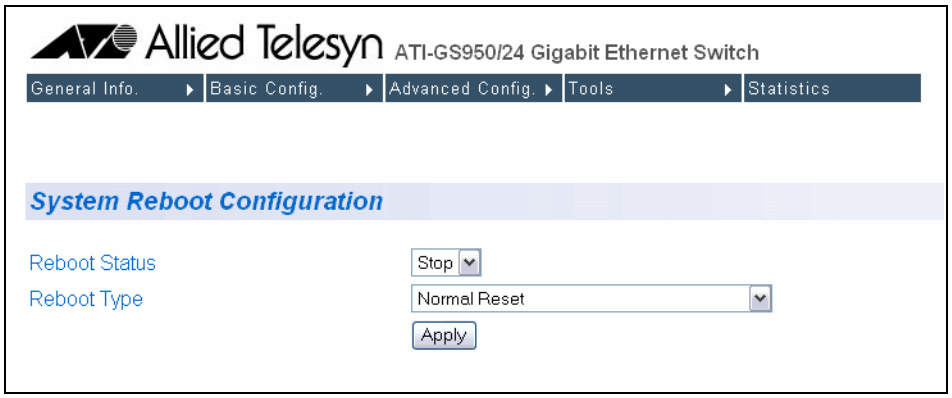


Figure 48. System Reboot Configuration Page

2. For the Reboot Type, select **Normal Reset**.This is the default setting.

   Note
   The two Reboot Type options **Reset to Factory Default** and are **Reset to Factory Default Except IP Address** are described in "Returning the AT-S79 Management Software to the Factory Default Values" on page 178.

3. For the Reboot Status, select **Start** to start the reboot.

4. Click **Apply**. The switch immediately begins to reload the AT-S79 management software. This process takes approximately one minute to complete. You can not manage the device during the reboot. After the reboot is finished, you can log in again if you want to continue to manage the device.

Pinging a Remote System

This procedure instructs the switch to ping a node on your network. This procedure is useful in determining whether an active link exists between the switch and another network device. Note the following before performing the procedure:

- The switch where you are initiating the ping must have an IP address.
- The device you are pinging must be a member of the Default VLAN. This means that the port on the switch through which the node is communicating with the switch must be an untagged or tagged member of the Default VLAN.

To ping a network device, perform the following procedure:

1. From the Tools menu, select **Ping**.

   The Ping Test Configuration page is shown in Figure 49.

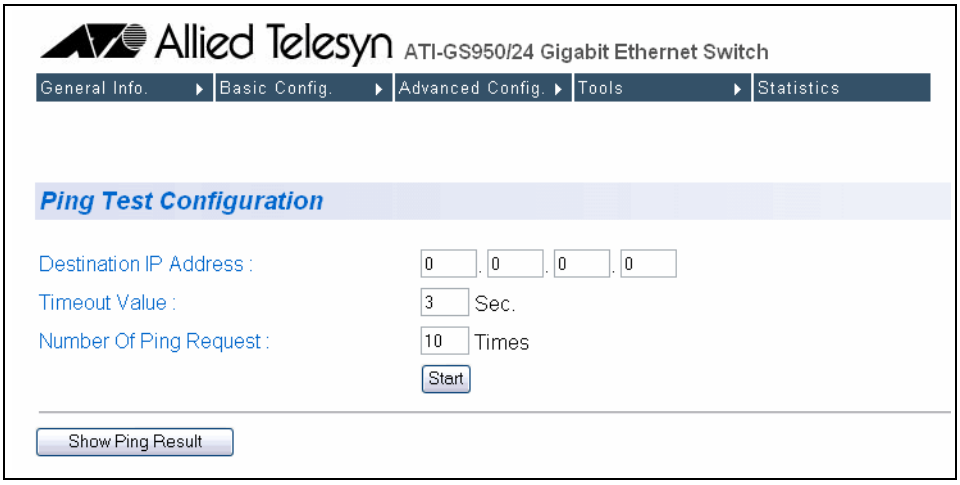


Figure 49. Ping Test Configuration Page

2. Configure the following parameters:

   Destination IP Address
   The IP address of the node you want to ping.

   Timeout Value
   Specifies the length of time in seconds the switch waits for a response before assuming that a ping has failed. The default is 3 seconds.

   Number of Ping Requests
   Specifies the number of ping requests you want the switch to perform. The default is 10.

3. Click **Start**.

4. To view the ping results, click **Show Ping Results**.

   A sample Ping Test Results page is shown in Figure 50.

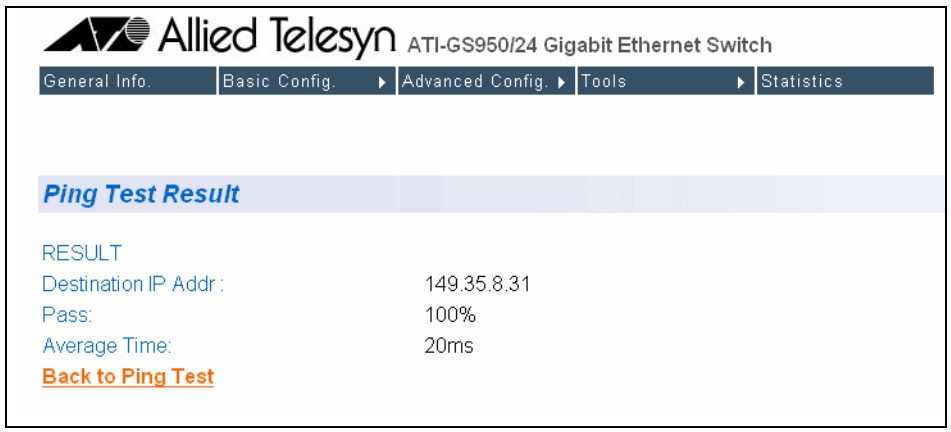


Figure 50. Ping Test Results Page

5. Click **Back to Ping Test** to return to the Ping Test Configuration page.

Returning the AT-S79 Management Software to the Factory Default Values

This procedure returns all AT-S79 management software parameters to their default values and deletes all tagged and port-based VLANs on the switch. The AT-S79 management software default values are listed in Appendix A, “AT-S79 Software Default Settings” on page 237.

Caution
This procedure causes the switch to reboot. The switch does not forward network traffic during the reboot process. Some network traffic may be lost.

To return the AT-S79 management software to the default settings, perform the following procedure:

1. From the Tools menu, select **System Reboot**.

   The System Reboot Configuration page is shown in Figure 48 on page 175.

2. For the Reboot Type, select one of the following:

   Reset to Factory Default
   Resets all switch parameters to the factory default settings, including IP address, subnet mask, and gateway address.

   Reset to Factory Default Except IP Address
   Resets all switch parameters to the factory default settings, but retains the IP address, subnet mask, and gateway settings. If the DHCP client is enabled, it remains enabled after this reset.

3. For the Reboot Status, select **Start** to start the reboot.

4. Click **Apply**.

   The switch is rebooted. You must wait for the switch to complete the reboot process before reestablishing your management session.

Chapter 16

Port Configuration

The sections in this chapter explain the two methods to viewing and changing the parameter settings of the individual ports on the switch. The first method shows how to use the Port Configuration page to view and configure multiple ports at one time. The second is typically used to configure just one port at a time. There is also a section for viewing port statistics. The sections are:

Viewing and Configuring Ports Using the Port Configuration Page

This procedure explains how to configure the ports on the switch using the Port Configuration page. This page allows you to view and configure the parameter settings of all the switch ports at one time.

To configure the ports, perform the following procedure:

1. From the Basic Config menu, select **Port Config**.

   The Port Configuration page is shown in Figure 51. The page lists all the ports on the switch and their current settings.

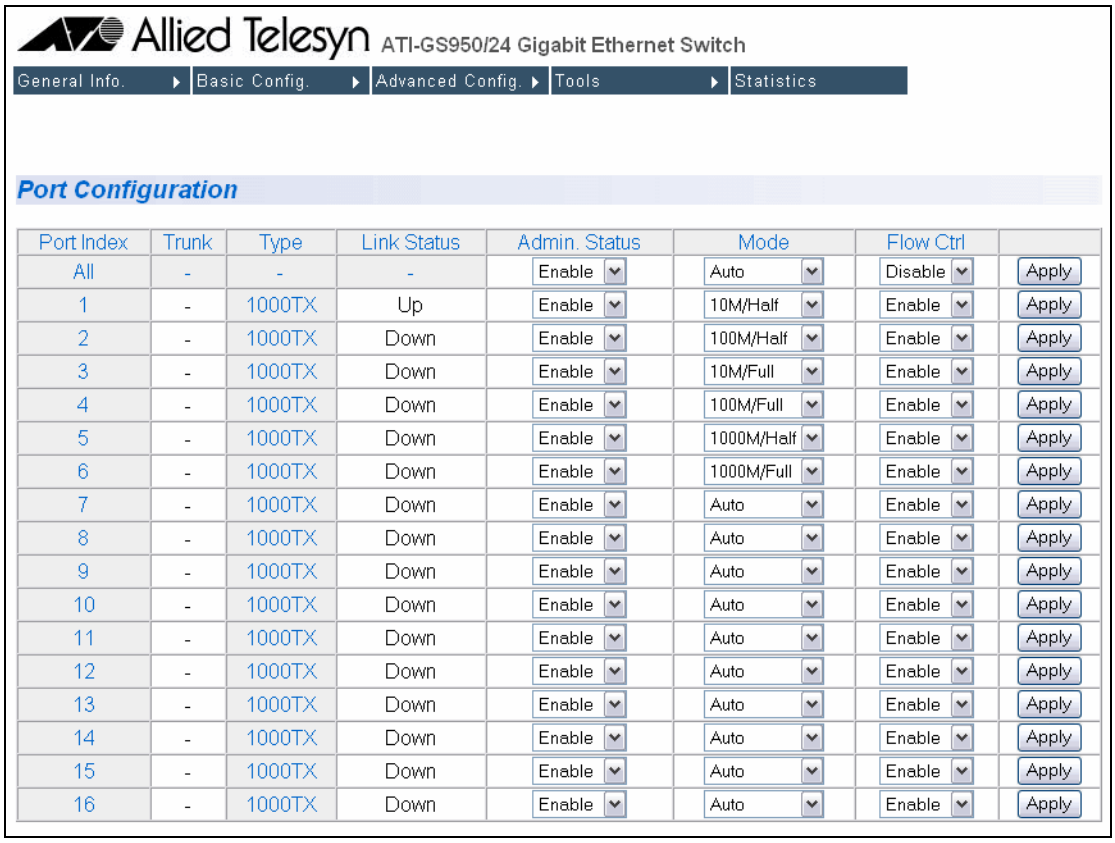


Figure 51. Port Configuration Page

2. Adjust the port settings as needed. Not all parameters are adjustable. The parameters are defined here:

   Port Index
   The port number. You cannot change this parameter.

   Trunk
   The trunk group number. A number in this column indicates that the port has been added to a trunk. For information about configuring a trunk, refer to Chapter 17, “Port Trunking” on page 189.

Type
The port type. The port type is 1000TX for 10/100/1000Base-T twisted pair ports and 1000BaseF for an optional SFP fiber port.

Link Status
The status of the link between the port and the end node connected to the port. The possible values are:

Up - A valid link exists between the port and the end node.

Down - The port and the end node have not established a valid link.

Admin. Status
The operating status of the port.

You can use this parameter to enable or disable a port. You may want to disable a port and prevent packets from being forwarded if a problem occurs with the node or cable connected to the port. After the problem has been fixed, you can enable the port to resume normal operation. You can also disable an unused port to secure it from unauthorized connections. The possible values are:

Enabled - The port is able to send and receive Ethernet frames. This is the default setting for a port.

Disabled - The port is disabled.

Mode
The speed and duplex mode settings for the port.

You can use this parameter to set the speed and duplex mode of a port. Possible settings are:

Auto - The port is using Auto-Negotiation to set the operating speed and duplex mode. This is the default setting for all ports. The actual operating speed and duplex mode of the port are displayed in parentheses (for example, "1000F" for 1000 Mbps full duplex mode) after a port establishes a link with an end node.

10M/Half - 10 Mbps in half-duplex mode

10M/Full - 10 Mbps in full-duplex mode

100M/Half - 100 Mbps in half-duplex mode

100M/Full - 100 Mbps in full-duplex mode

1000M/Half - 1000 Mbps in half-duplex mode

1000M/Full - 1000 Mbps in full-duplex mode

When selecting a setting, note the following:

- When a twisted pair port is set to Auto-Negotiation, the default setting, the end node should also be using Auto-Negotiation to

prevent a duplex mode mismatch. A switch port using Auto-Negotiation defaults to half-duplex if it detects that the end node is not using Auto-Negotiation. This can result in a mismatch if the end node is operating at a fixed duplex mode of full-duplex. To avoid this problem when connecting an end node with a fixed duplex mode of full-duplex to a switch port, disable Auto-Negotiation on the port and set the port's speed and duplex mode manually.

- Allied Telesyn does not recommend manually setting a 10/100/1000Base-T twisted pair port to either 1000 Mbps full duplex or 1000 Mbps half duplex. For 1000 Mbps operation, Allied Telesyn recommends setting the port to Auto-Negotiation.
- The only valid setting for an optional SFP port is Auto-Negotiation.

Flow Control
The current flow control setting on the port. The switch uses a special pause packet to notify the end node to stop transmitting for a specified period of time. The possible values are:

Enabled - The port is allowed to use flow control. This is the default setting for all ports on the switch.

Disabled - The port does not use flow control.

3. Click **Apply** to save the configuration.

Viewing and Configuring Ports Using the Configuration of Port Page

The procedure in this section is used to view or configure the parameter settings of a port on the switch. To view and configure the parameter settings for more than one port at a time, refer to "Viewing and Configuring Ports Using the Port Configuration Page" on page 180.

To view or configure the parameter settings of a port, perform the following procedure:

1. From the home page, click the port that you want to configure in the graphical image of the switch.

   The management software displays the Configuration of Port menu. This menu displays the current parameter settings of the selected port. An example of the menu is shown in Figure 52.

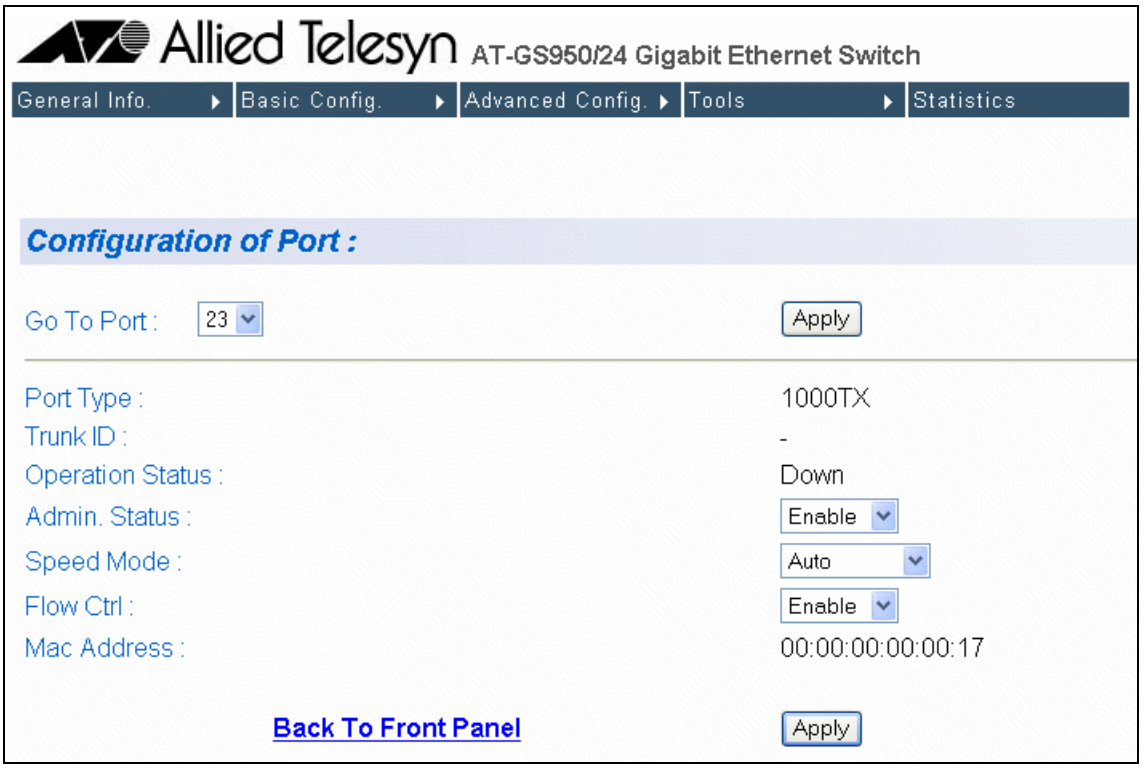


Figure 52. Configuration of Port Page

2. Adjust the port settings as needed. Not all parameters are adjustable. The parameters are defined here:

   Port Index
   The port number. You cannot change this parameter.

Port Type
The port type. The port type is 1000TX for 10/100/1000Base-T twisted pair ports and 1000BaseF for an optional SFP fiber optic port.

Trunk ID
The trunk group number. A number in this column indicates that the port is a member of a port trunk. For information about configuring a trunk, refer to Chapter 17, “Port Trunking” on page 189.

Operational Status
The status of the link between the port and the end node connected to the port. The possible values are:

Up - A valid link exists between the port and the end node.

Down - The port and the end node have not established a valid link.

Admin. Status
The operating status of the port.

You can use this parameter to enable or disable a port. You may want to disable a port and prevent packets from being forwarded if a problem occurs with the node or cable connected to the port. After the problem has been fixed, you can enable the port to resume normal operation. You can also disable an unused port to secure it from unauthorized connections. The possible values are:

Enabled - The port is able to send and receive Ethernet frames. This is the default setting for a port.

Disabled - The port is disabled.

Speed Mode
The speed and duplex mode settings for the port.

You can use this parameter to set the speed and duplex mode of a port. Possible settings are:

Auto - The port is using Auto-Negotiation to set the operating speed and duplex mode. This is the default setting for all ports. The actual operating speed and duplex mode of the port are displayed in parentheses (for example, “1000F” for 1000 Mbps full duplex mode) after a port establishes a link with an end node.

10M/Half - 10 Mbps in half-duplex mode

10M/Full - 10 Mbps in full-duplex mode

100M/Half - 100 Mbps in half-duplex mode

100M/Full - 100 Mbps in full-duplex mode

1000M/Half - 1000 Mbps in half-duplex mode

1000M/Full - 1000 Mbps in full-duplex mode

When selecting a setting, note the following:

- When a twisted pair port is set to Auto-Negotiation, the default setting, the end node should also be using Auto-Negotiation to prevent a duplex mode mismatch. A switch port using Auto-Negotiation defaults to half-duplex if it detects that the end node is not using Auto-Negotiation. This can result in a mismatch if the end node is operating at a fixed duplex mode of full-duplex. To avoid this problem when connecting an end node with a fixed duplex mode of full-duplex to a switch port, disable Auto-Negotiation on the port and set the port's speed and duplex mode manually.
- Allied Telesyn does not recommend manually setting a 10/100/1000Base-T twisted pair port to either 1000 Mbps full duplex or 1000 Mbps half duplex. For 1000 Mbps operation, Allied Telesyn recommends setting the port to Auto-Negotiation.
- The only valid setting for an optional SFP port is Auto-Negotiation.

Flow Control
The current flow control setting on the port. The switch uses a special pause packet to notify the end node to stop transmitting for a specified period of time. The possible values are:

Enabled - The port uses flow control. This is the default setting for all ports on the switch.

Disabled - The port does not use flow control.

MAC Address
The port's MAC address. This setting can not be changed.

3. Click **Apply**.

4. To view or configure the parameter settings on another port, do the following:

   a. Click **Go to Port** and select the port from the pull-down menu,

   b. Click **Apply**.

   c. Configure the parameters as needed. Refer to Step 2 in this procedure for definitions of the parameters.

Displaying Port Statistics

To display port statistics, perform the following procedure:

1. Select **Statistics**.

   The Statistics page opens as shown in Figure 53.

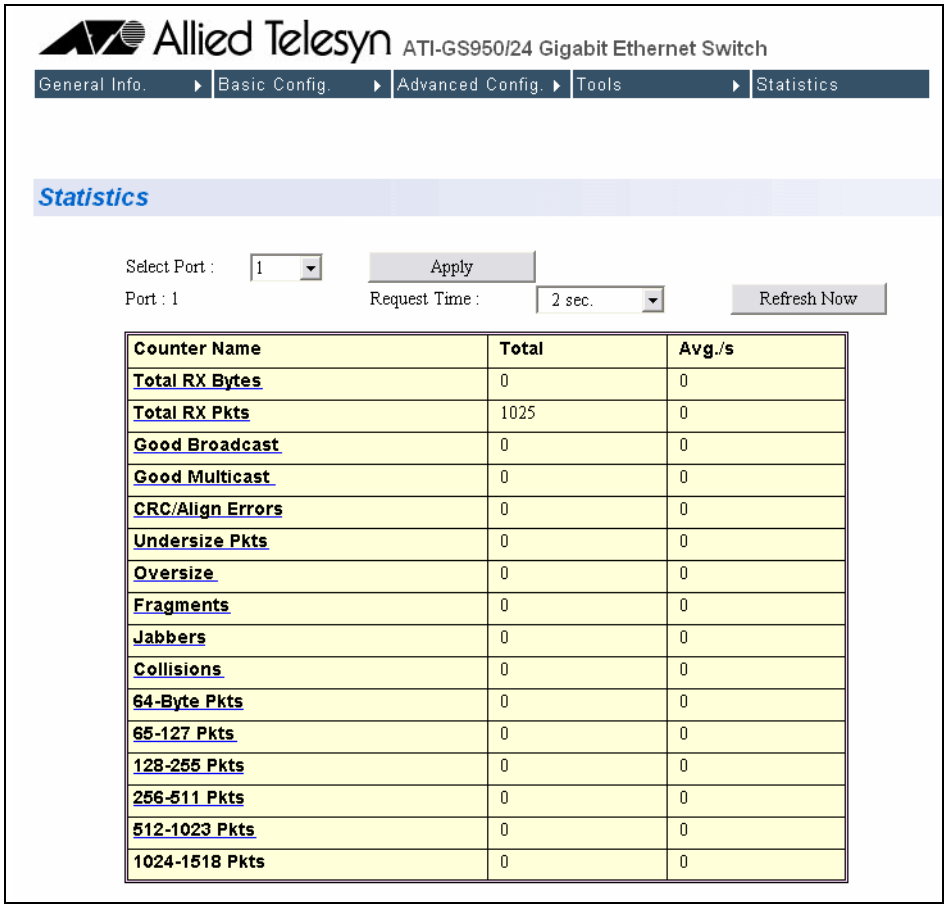


Figure 53. Statistics Page

2. To view statistics for a port, select a port from the Select Port pull-down menu and click **Apply**.

   The statistics are displayed in a table that contains the following items of information:

   Total RX Bytes
   Number of bytes received on the port.

   Total RX Packets
   Number of packets received on the port.

Good Broadcast
Number of valid broadcast packets received on the port.

Good Multicast
Number of valid multicast packets received on the port.

CRC/Align Errors
Number of packets with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received on the port.

Undersize Packets
Number of packets that were less than the minimum length specified by IEEE 902.3 (64 bytes including the CRC) received on the port.

Oversize Packets
Number of packets that exceeded the maximum length specified by IEEE 902.3 (1518 bytes including the CRC) received on the port.

Fragments
Number of undersized packets, packets with alignment errors, and packets with FCS errors (CRC errors) received on the port.

Jabbers
Number of electrical signal errors detected on the port.

Collisions
Number of packet collisions on the port.

64-Byte Pkts
Number of 64-byte packets sent or received by the port. The minimum length of an Ethernet packet is 64 bytes.

65-127 Pkts
Number of 65- to 127-byte packets sent or received by the port.

128-255 Pkts
Number of 128- to 255-byte packets sent or received by the port.

256-511 Pkts
Number of 256- to 511-byte packets sent or received by the port.

512-1023 Pkts
Number of 512- to 1023-byte packets sent or received by the port.

1023-1518 Pkts
Number of 1023- to 1518-byte packets sent or received by the port. The maximum length of an Ethernet packet is 1518 bytes.

3. To modify how frequently the statistics are updated, from the Request Time pull-down menu select the desired time and click **Refresh Now**. The default is every two seconds. (The Refresh Now button can be used at any time to update the page.)

Chapter 17
Port Trunking

This chapter contains the following procedures for working with port trunking:

Note
For background information, refer to “Port Trunking Overview” on page 58.

Creating a Port Trunk

This procedure explains how to create a port trunk.

Note
Do not connect the cables of a port trunk to the ports on the switch until after you have configured the ports on both the switch and the end node. Connecting the cables prior to configuring the ports can create loops in your network topology. Loops can result in broadcast storms, which can adversely affect the operation of your network.

To create a port trunk, perform the following procedure:

1. From the **Advanced Config** menu, select **Trunk Config**.

   The Trunk Configuration page is shown in Figure 54.

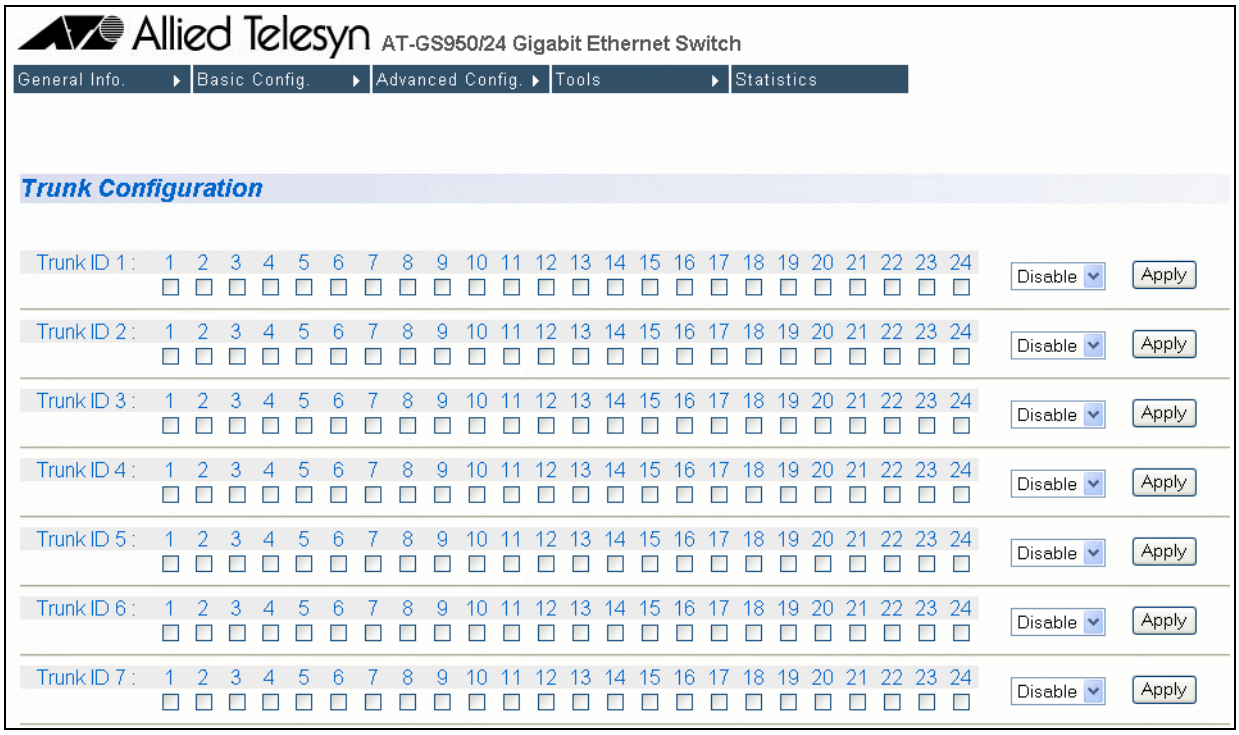


Figure 54. Trunk Configuration Page

If the switch does not contain a port trunk, all of the ports on the switch are unchecked. If there is a port trunk, the ports in the trunk are checked.

2. In any one of the unused Trunk ID rows, click the dialog boxes of the ports that will make up the port trunk. A check in a box indicates the port is a member of the trunk. No check means the port is not a member. A port trunk can contain up to eight ports.

3. Change the status of the trunk from **Disable** to **Enable**.

4. Click **Apply**.

   The trunk is now operational on the switch.

5. Configure the port trunk on the other switch and connect the cables.

Modifying a Port Trunk

This procedure adds and removes ports from a port trunk.

> **Note**
> You should disconnect the cables from the ports of the trunk on the switch before modifying it. Adding or removing ports from a trunk without first disconnecting the cables can create loops in your network topology, which can cause broadcast storms and poor network performance.

To add or remove ports from a trunk, perform the following procedure:

1. From the **Advanced Config** menu, select **Trunk Config**.

   The Trunk Configuration page is shown in Figure 54.

2. Click the status of the port trunk to be modified and change the status from Enable to Disable.

   > **Note**
   > Allied Telesyn recommends disabling a port trunk before adding or removing ports.

3. Click **Apply**.

4. To add or remove a port from a trunk, click the dialog box for the port in the corresponding trunk row. A check in a box indicates the port is a member of the trunk. No check means the port is not a member.A port trunk can contain up to eight ports.

5. Click **Apply**.

6. Modify the port trunk on the other switch and reconnect the cables.

Enabling and Disabling a Port Trunk

This procedure enables and disables a port trunk. Note the following before performing this procedure:

- Do not enable a port trunk until after you have configured the trunk on both switches.
- Do not connect the cables to the ports on the switches until after you have configured and enabled the trunk on both switches.

> **Note**
> If you are disabling a port trunk, be sure to first disconnect all cables from the ports of the trunk. Leaving the cables connected can create loops in your network topology because the ports of a disabled port trunk function as normal network ports, forwarding individual network traffic.

To enable or disable a port trunk, perform the following procedure:

1. From the **Advanced Config** menu, select **Trunk Config**.

   The Trunk Configuration page is shown in Figure 54.

2. Click the status of the port trunk and change it to **Enable** or **Disable**.
3. Click **Apply**.

Chapter 18
Port Mirroring

This chapter contains the procedure for setting up port mirroring. Port mirroring allows you to unobtrusively monitor the ingress and egress traffic on a port by having the traffic copied to another port. This chapter contains the following sections:

Note
For background information, refer to “Port Mirroring Overview” on page 66.

Configuring Port Mirroring

To set up port mirroring, perform the following procedure:

1. From the **Advanced Config** menu, select **Port Mirroring**.

   The Port Mirroring page is shown in Figure 55.

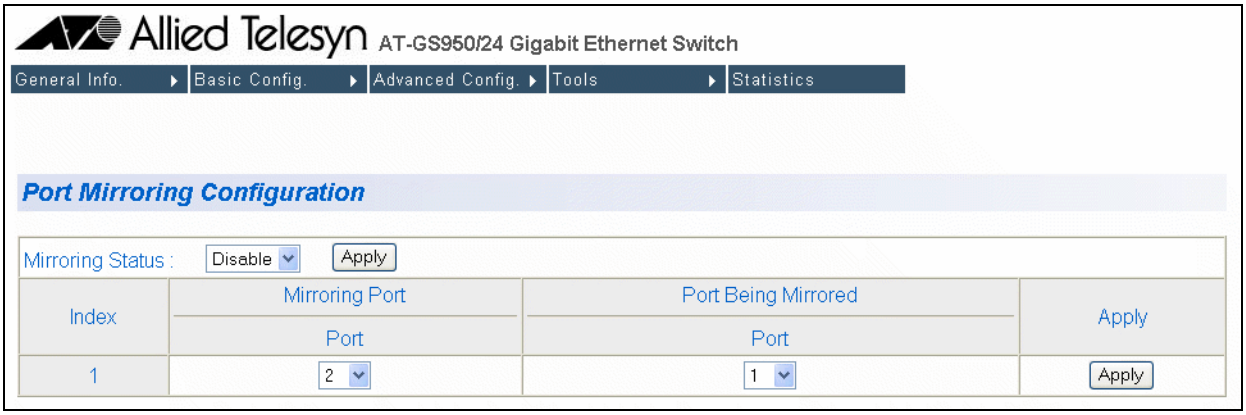


Figure 55. Port Mirroring Page

2. In the Mirroring Port section, click **Port** and from the pull-down menu select the port where the network analyzer is connected.

3. In the Port Being Mirrored section, click **Port** and from the pull-down menu select the port whose ingress and egress traffic you want to monitor. You can select only one port.

4. Click **Apply** on the right-hand side of the page.

5. From the Mirroring Status list, select **Enable** and click **Apply**.

   Port mirroring is immediately enabled on the switch. You can now connect a data analyzer to the mirroring port to monitor the traffic on the other port.

Disabling Port Mirroring

To disable port mirroring, perform the following procedure:

1. From the **Advanced Config** menu, select **Port Mirroring**.

   The Port Mirroring page is shown in Figure 55 on page 196.

2. From the Mirroring Status list, select **Disable** and click **Apply**.

   Port mirroring is immediately disabled on the switch. You can now use the mirroring port for regular network operations.

Chapter 19

Virtual LANs

This chapter contains the procedures for creating, modifying, and deleting port-based and tagged Virtual Local Area Networks (VLANs) from a web browser management session. This chapter contains the following sections:

Note
For background information, refer to “Port-based VLAN Overview” on page 74 and “Tagged VLAN Overview” on page 80.

Creating a VLAN

This section contains the procedure for creating a new port-based or tagged VLAN. This procedure assigns the VLAN a name, a VID number, and the untagged and tagged member ports.

After performing this procedure, the PVID values of the untagged ports of the VLAN must be adjusted to match the virtual LAN's VID number. In order for a port to be considered an untagged member of a VLAN, its PVID value must be changed to match the VID of the virtual LAN. This procedure is found in "Configuring the PVID of Untagged Ports" on page 202.

To configure a VLAN, perform the following procedure:

1. From the **Advanced Config** menu, select **VLAN Config** and then **Create VLAN**.

   The Create VLAN page is shown in Figure 56.

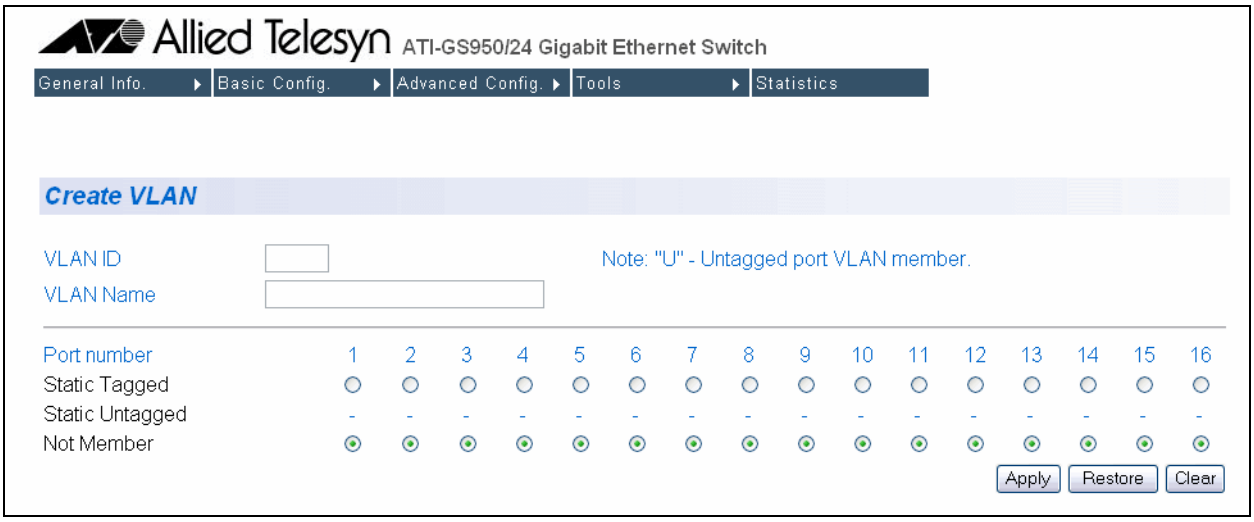


Figure 56. Create VLAN Page

2. Click the **VLAN ID** field and enter a VLAN ID for the new VLAN. The range is 2 to 4094.

   If this VLAN will be unique in your network, then its VLAN ID (VID) must also be unique from all other VIDs in the network.

3. In the VLAN Name field, enter a name for the VLAN.

   The name can contain up to 32 characters including spaces but not including special characters such as asterisks (*) or exclamation points (!).

If the VLAN will be unique in you network, then the name should be unique as well.

If the VLAN will be part of a larger VLAN that spans multiple switches, then the name for the VLAN should be the same on each switch where nodes of the VLAN are connected.

4. In the Static Tagged row, click the dialog circles of those ports on the switch that are to be tagged or untagged members of the new VLAN.

   While you might assume that the Static Tagged row should only be used to specify tagged ports of the VLAN, it should be used to specify the untagged ports of a new VLAN as well.

5. Click **Apply** to create the new VLAN.

   The switch creates the VLAN. However, the window does not change. It continues to display the VLAN just created.

6. To create a new VLAN, click **Clear** or repeat this procedure.

7. If the new VLAN contains untagged ports, perform the next procedure, "Configuring the PVID of Untagged Ports" on page 202, to change the PVID of the untagged ports to match the virtual LAN's VID.

Configuring the PVID of Untagged Ports

This procedure adjusts a port's VID value. The PVID value determines the VLAN in which the port is an untagged member. A port is an untagged member of the VLAN whose VID value matches its PVID. A port can be an untagged member of only one VLAN at a time.

The ports of a new VLAN are initially designated as tagged ports. Their PVID values retain their previous settings when they are assigned to a new VLAN. If you want the ports to function as untagged members of a new VLAN, you must change their PVID values to match the VID of the VLAN, as explained in this procedure.

You can also use this procedure to change the VLAN assignment of an untagged port. With this procedure you can move an untagged port from one VLAN to another by changing its PVID value.

To adjust the PVID value of a port, perform the following procedure:

1. From the **Advanced Config** menu, select **VLAN Config** and then **VLAN Port Config**.

   The VLAN Port Configuration page is shown in Figure 57.

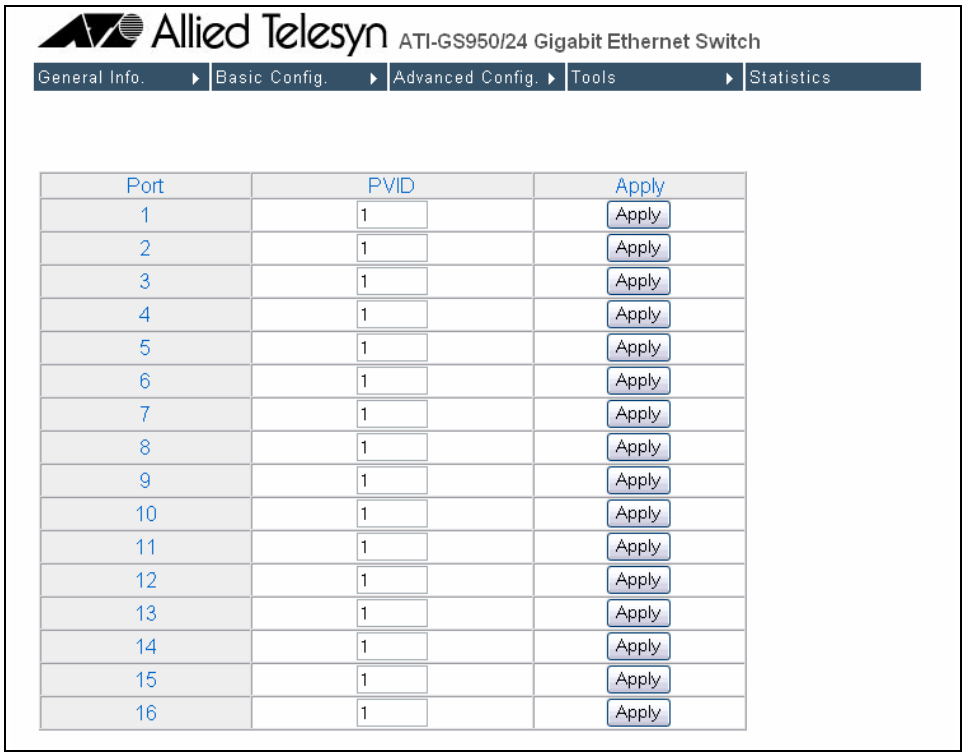


Figure 57. PVID Page

2. Click the **PVID** field of the port whose value you want to change and enter the new PVID value for the port. The PVID must be equal to the VID of the VLAN where you want the port to be an untagged member.

   For example, to make Port 10 an untagged member of a VLAN that has a VID of 12, you would change its PVID to 12.

   Note
   If you specify a PVID that does not correspond to any VIDs on the switch, the management software creates a new VLAN with a VID that equals the PVID. The VLAN is not assigned any name.

3. Click **Apply**.

4. Repeat steps 2 and 3 to change the PVID values of other ports.

Displaying the VLANs

To display the VLANs, perform the following procedure:

1. From the **Advanced Config** menu, select **VLAN Config** and then **VLAN Port Config**.

   The VLAN Information page is shown in Figure 59 on page 205 and provides the following columns of information:

   VLAN ID
   The VLAN ID number.

   Name
   The VLAN's name.

   VLAN Type
   The VLAN type as either permanent or static. The Default VLAN is permanent and port-based and tagged VLANs are static.

2. To view the ports of a VLAN, click the VID of the VLAN.

   An example of the VLAN Configuration - Members page is shown in Figure 58.

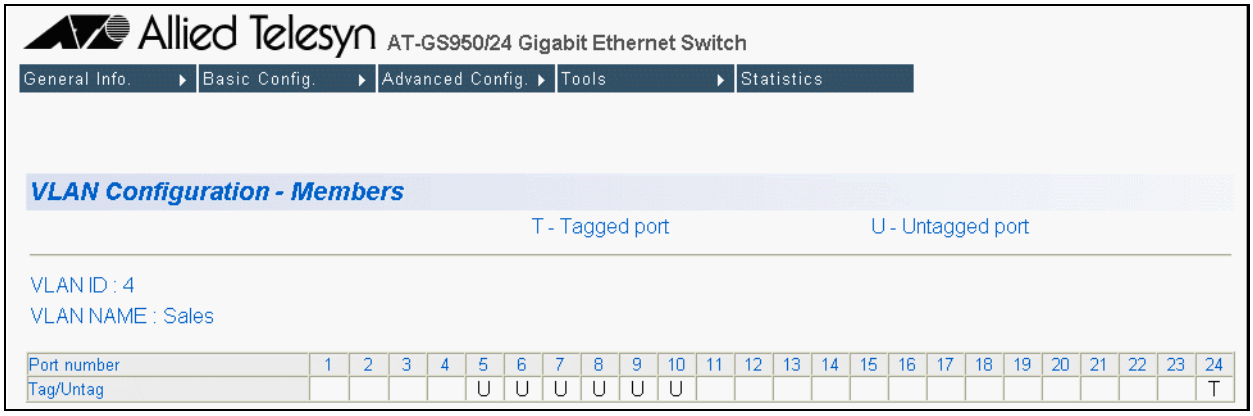


Figure 58. VLAN Configuration - Members Page

Untagged ports of the VLAN are indicated with a "U" and tagged ports with a "T".

Modifying a VLAN

This procedure allows you to perform the following functions:

- Change the name of a VLAN.
- Add or remove tagged ports from a VLAN.

Before performing this procedure, note the following:

- You cannot change the VID of an existing VLAN.
- You cannot add an untagged port to a VLAN using this procedure. That function requires changing a port's VID value, as explained in "Configuring the PVID of Untagged Ports" on page 202
- You cannot remove an untagged port from a VLAN using this procedure. To remove an untagged port from a VLAN, you must assign it as an untagged member of another VLAN by changing its PVID, as explained in "Configuring the PVID of Untagged Ports" on page 202.

To change the name of a VLAN or to add or remove tagged ports, perform the following procedure:

1. From the **Advanced Config** menu, select **VLAN Info**.

   The VLAN Information page is shown in Figure 59.

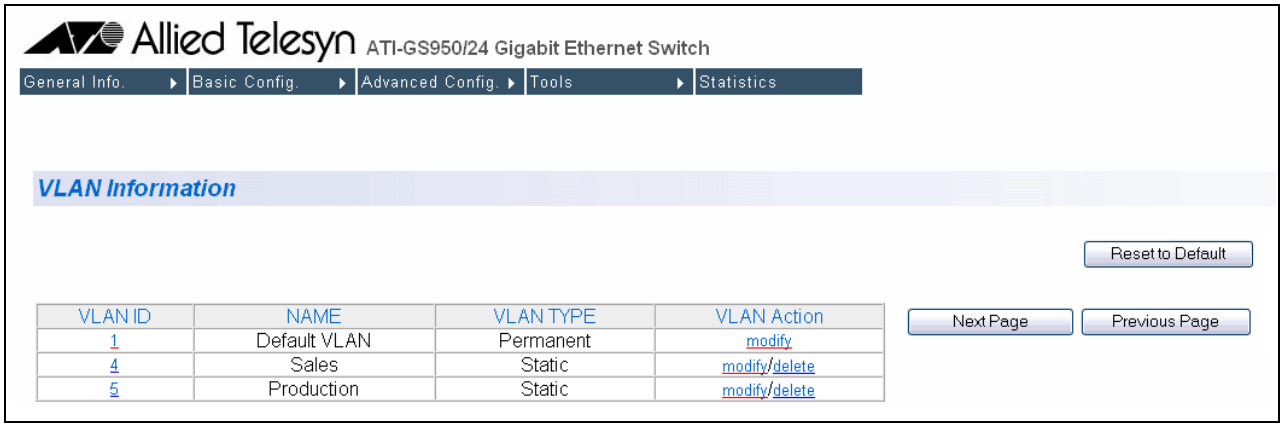


Figure 59. VLAN Information Page

   Use the **Next Page** and **Previous Page** buttons to scroll through the list of VLANs.

2. In the VLAN Action column, click **Modify** next to the VLAN you want to modify.

The Modify VLAN page is shown in Figure 60.

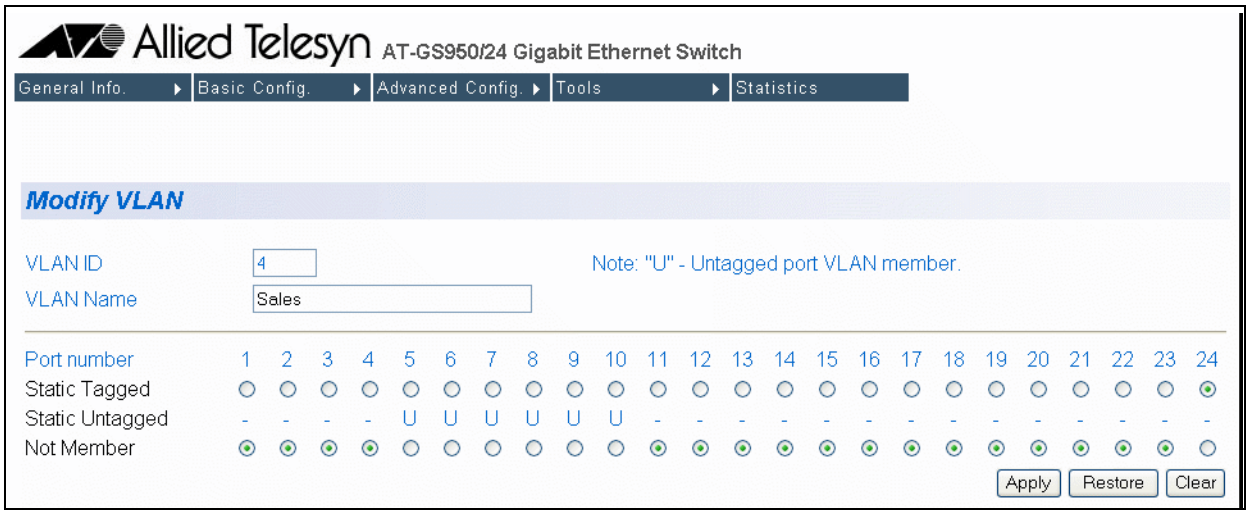


Figure 60. Modify VLAN Page

3. To change the VLAN's name, click the VLAN Name field and enter the new name.

   The name can contain up to 32 characters including spaces but not including special characters such as asterisks (*) or exclamation points (!).

4. To add a new tagged port to the VLAN, click the dialog circle in the Static Tagged row of the port to be added as a tagged port.

5. To remove a tagged port from the VLAN, click the dialog circle in the Not Member row of the port to be removed.

   If you make changes to the VLAN that you want to cancel, click **Restore**. If you want to clear the current name and all tagged port assignments from the VLAN prior to assigning it a new name and new tagged ports, click **Clear**.

6. After you have made the desired changes, click **Apply**.

   The changes are implemented on the VLAN. The current VLAN window remains on the screen. You can make additional changes to the VLAN or you can repeat this procedure to modify other VLANs.

Deleting a VLAN

To delete a VLAN, perform the following procedure:

1. From the **Advanced Config** menu, select **VLAN Info**.

   The VLAN Information page is shown in Figure 59 on page 205.

2. In the VLAN Action column, click **Delete** next to the VLAN you want to delete.

   A confirmation prompt is displayed.

3. Click **OK** to delete the VLAN or **Cancel** to cancel the deletion.

   Note
   You cannot delete the Default VLAN which has a VID of 1.

   The VLAN Information window is updated to show that the VLAN is deleted. The untagged ports of a deleted VLAN are automatically returned to the Default VLAN.

Chapter 20

Quality of Service (QoS)

This chapter contains the procedure for configuring Quality of Service (QoS). This chapter includes the following procedures:

Note
For background information, refer to “QoS Overview” on page 96

Mapping CoS Priorities to Egress Queues

This procedure explains how to change the default mappings of CoS priorities to egress priority queues, as shown in Table 2 on page 97. This is set at the switch level. You cannot set this at the per-port level. This procedure also enables and disables QoS.

To change the default mappings of CoS priorities to egress priority queues or to enable or disable QoS, perform the following procedure:

1. From the **Advanced Config** menu, select **QoS Config** and then select **QoS Config**.

   The QoS Configuration page is shown in Figure 61.

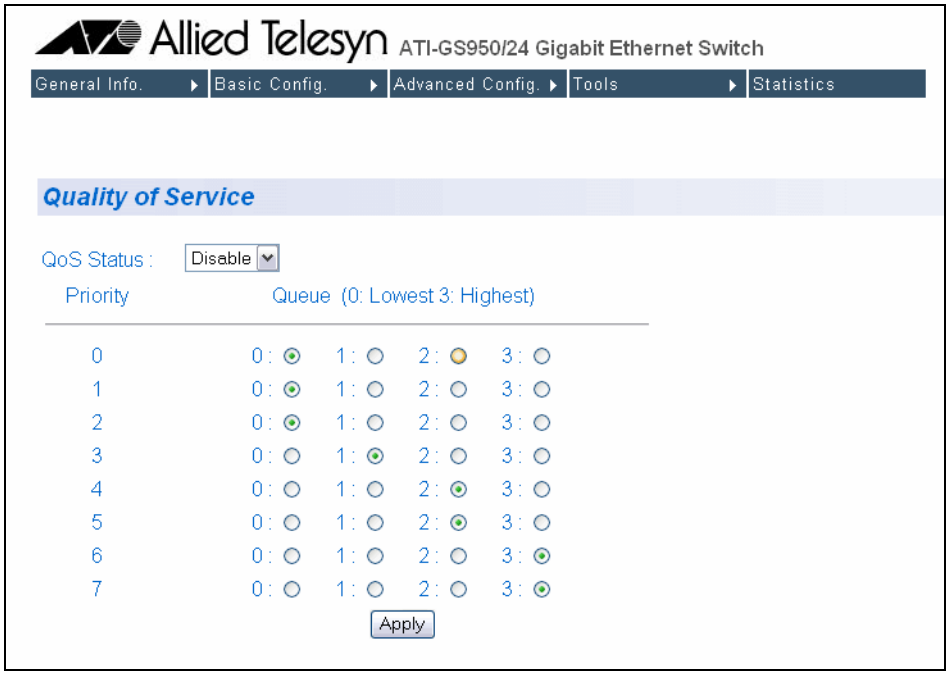


Figure 61. QoS Configuration Page

2. To enable or disable QoS, select **Enable** or **Disable** from the QoS Status pull-down menu. The default is disabled.

3. To change the egress priority queue assignment of an 802.1p priority class, click the dialog circle of the queue for the corresponding priority. For example, to direct all tagged traffic with a priority of 4 to egress queue 3 on the ports, you would click the dialog circle for queue 3 in the priority 4 row.

4. Click **Apply**.

Note

The switch does not alter the original priority level in tagged frames. Frames leave the switch with the same priority level they had when they entered the switch.

Configuring CoS

As explained in “QoS Overview” on page 96, a packet received on a port is placed it into one of four priority queues on the egress port according to the switch’s mapping of 802.1p priority levels to egress priority queues. The default mappings are shown in Table 2 on page 97.

You can override the mappings at the port level by assigning a new default egress queue to a port. Note that this assignment is made on the ingress port and before the frame is forwarded to the egress port. Consequently, you need to configure this feature on the ingress port. For example, you can configure a switch port so that all ingress frames are stored in egress queue 3 of the egress port, regardless of the priority levels that might be in the frames themselves, as found in tagged frames.

Note
The switch does not alter the original priority level in tagged frames. Frames leave the switch with the same priority level they had when they entered the switch.

To configure CoS for a port, perform the following procedure:

1. From the **Advanced Config** menu, select **QoS Config** and then select **Port Priority**.

   The Port Priority Configuration page is shown in Figure 62.

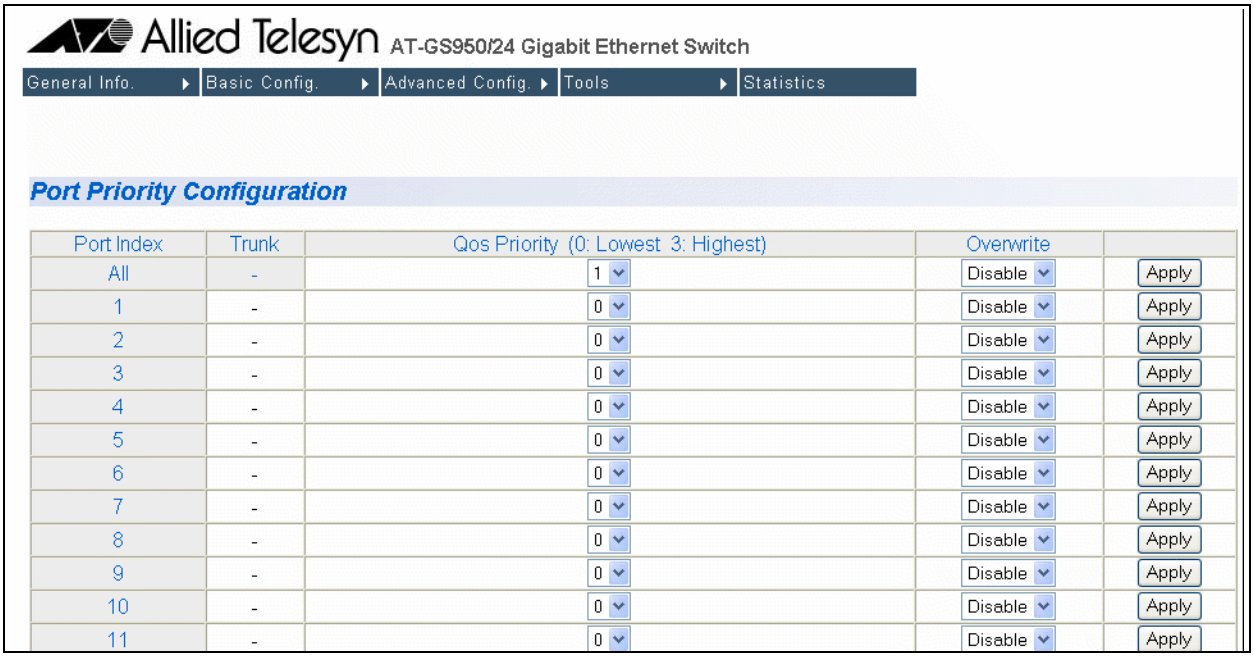


Figure 62. Port Priority Configuration Page

The columns in the menu display the following information:

Port
Displays the port number.

Trunk
Displays the trunk number if the port is a member of a trunk.

QoS Priority
Displays the number of the queue where untagged packets received on the port are stored on the egress queue.

Override
Displays whether the priority level in ingress tagged frames is being used or not. If No, the override is deactivated and the port is using the priority levels contained within the frames to determine the egress queue. If Yes, the override is activated and the tagged packets are stored in the egress queue specified in the Queue column.

2. To change the egress queue where ingress untagged frames received on a port are to be stored on the egress port, use the pull-down menu in the QoS Priority column and select the desired queue. The range is 0 (lowest) to 3 (highest). The default is 0. For example, if you select 3 for queue 3 for a port, all ingress untagged packets received on the port are stored in egress queue 3 on the egress port. (If you perform Step 3 and override the priority level in ingress tagged packets, this also applies to tagged packets as well.)

   If the selected port is part of a port trunk, all ports in the trunk are automatically assigned the same egress queue.

3. To configure a tagged port so that the switch ignores the priority tag in ingress tagged frames, select **Enable** from the Override column for the corresponding port.

   The default for this parameter is disabled, meaning that the priority level of tagged frames is determined by the priority level specified in the frame itself.

4. Click **Apply**.

Note
The tagged information in a frame is not changed as the frame traverses the switch. A tagged frame leaves a switch with the same priority level that it had when it entered.

Chapter 21

Rapid Spanning Tree Protocol (RSTP)

This chapter contains the following procedures for working with the Remote Spanning Tree Protocol (RSTP):

Note
For background information on RSTP, refer to “RSTP Overview” on page 108.

Basic RSTP Configuration

To configure the RSTP settings, perform the following procedure:

1. From the Basic Config menu, select **Rapid Spanning Tree** and then **RSTP Config**.

   The Rapid Spanning Tree Configuration page is shown in Figure 63.

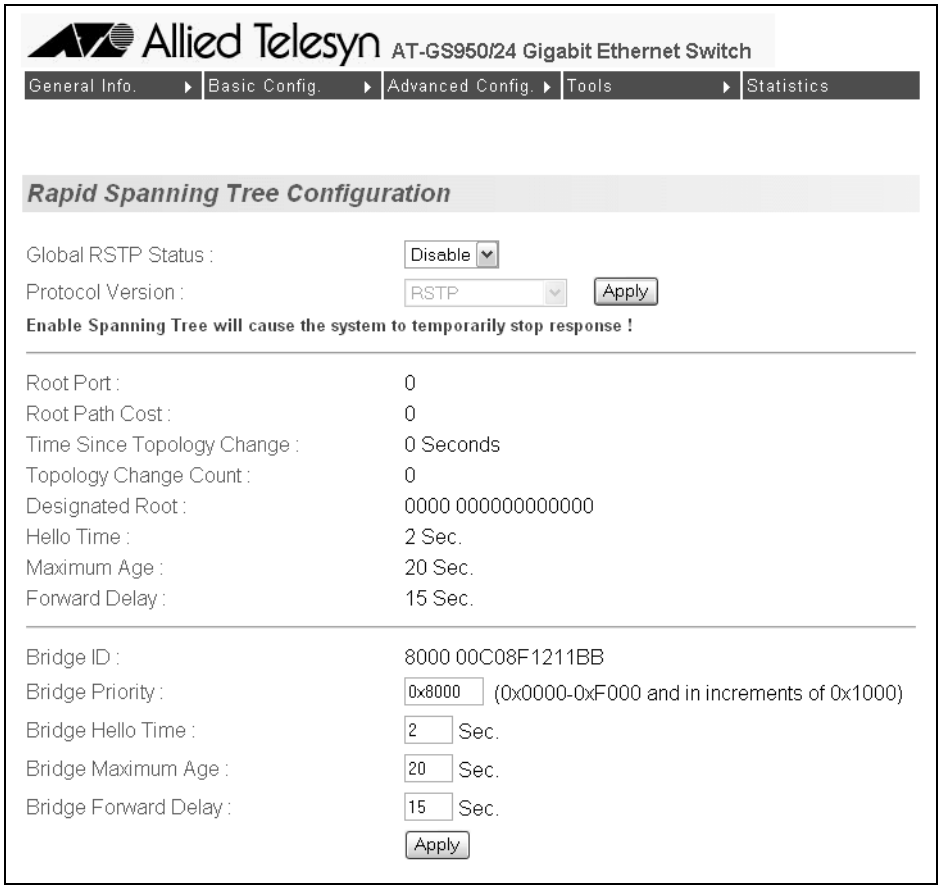


Figure 63. Rapid Spanning Tree Configuration Page

The RSTP Configuration page allows you to configure RSTP as well as to view the current settings and contains the following items of information in the middle portion:

Root Port
The active port on the switch that is communicating with the root bridge. If the switch is the root bridge for the LAN, then there is no root port and the root port parameter will be 0.

Root Path Cost
The sum of all the root port costs of all the bridges between the

switch's root port and the root bridge including the switch's root port cost.

Time Since Topology Change
The time in seconds since the last topology change took place. When RSTP detects a change to the LAN's topology or when the switch is rebooted, this parameter is reset to 0 seconds and begins incrementing until the next topology change is detected.

Topology Change Count
An integer that reflects the number of times RSTP has detected a topology change on the LAN since the switch was initially powered on or rebooted.

The following parameters refer to the designated root bridge:

Designated Root
This parameter includes two fields: the root bridge priority and the MAC address of the root bridge. For example, 1000 00C08F1211BB shows the root bridge priority as 1000, and 00C08F1211BB as the MAC address.

Hello Time
The hello time. See "Hello Time and Bridge Protocol Data Units (BPDUs)" on page 111. This parameter affects only the root bridge.

Maximum Age
The maximum amount of time that BPDUs are stored before being deleted on the root bridge.

Forward Delay
The time interval between generating and sending configuration messages by the root bridge.

The lower section provides information about the bridge:

The following parameters refer to the switch.

Bridge ID
The MAC address of the bridge. The bridge identifier is use as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority. You cannot change this setting.

Bridge Hello Time
This is the time interval between generating and sending configuration messages by the bridge. This parameter is active only when the switch is the root bridge.

Bridge Maximum Age
The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge.

Bridge Forward Delay
This is the time interval between generating and sending configuration messages by the bridge.

Configuring RSTP Port Settings

This section contains the following topics:

Configuring the Basic RSTP Port Settings

To configure the basic RSTP port settings, perform the following procedure:

1. From the Basic Config menu, select **Rapid Spanning Tree** and then **RSTP Basic Port Config**.

   The RSTP Basic Port Configuration page is shown in Figure 64.

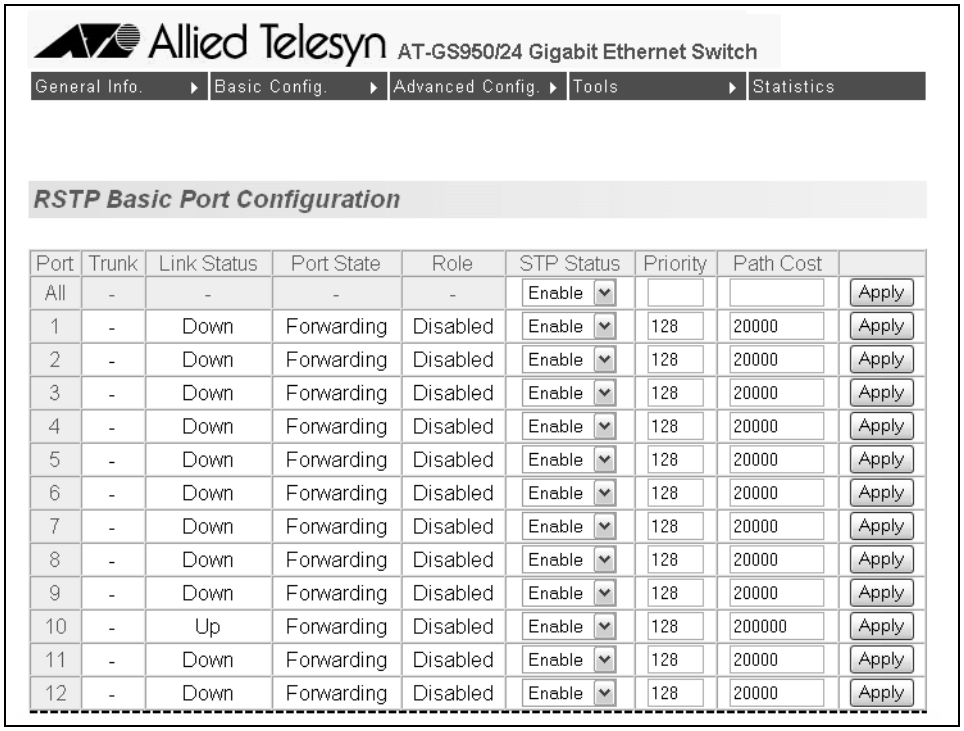


Figure 64. RSTP Basic Port Configuration Page

2. In the STP Status column for the port you want to configure, select the STP status from the list, either Enable or Disable.

3. In the Priority column for the port you want to configure, type a number for the port priority.

   Port priority is described in "Port Priority" on page 110.

4. In the Path Cost column for the port you want to configure, type a number for the Path Cost.

Path cost is described in “Path Costs and Port Costs” on page 109.

5. Click **Apply**.

6. To configure all of the ports to the same settings, in the All row, configure one, two, or all of the following settings: STP Status, Priority, and Path Cost. Click **Apply**.

Configuring the Advanced RSTP Port Settings

To configure the advanced RSTP port settings, perform the following procedure:

1. From the Basic Config menu, select **Rapid Spanning Tree** and then **RSTP Adv. Port Config**.

The RSTP Advanced Port Configuration page is shown in Figure 65.

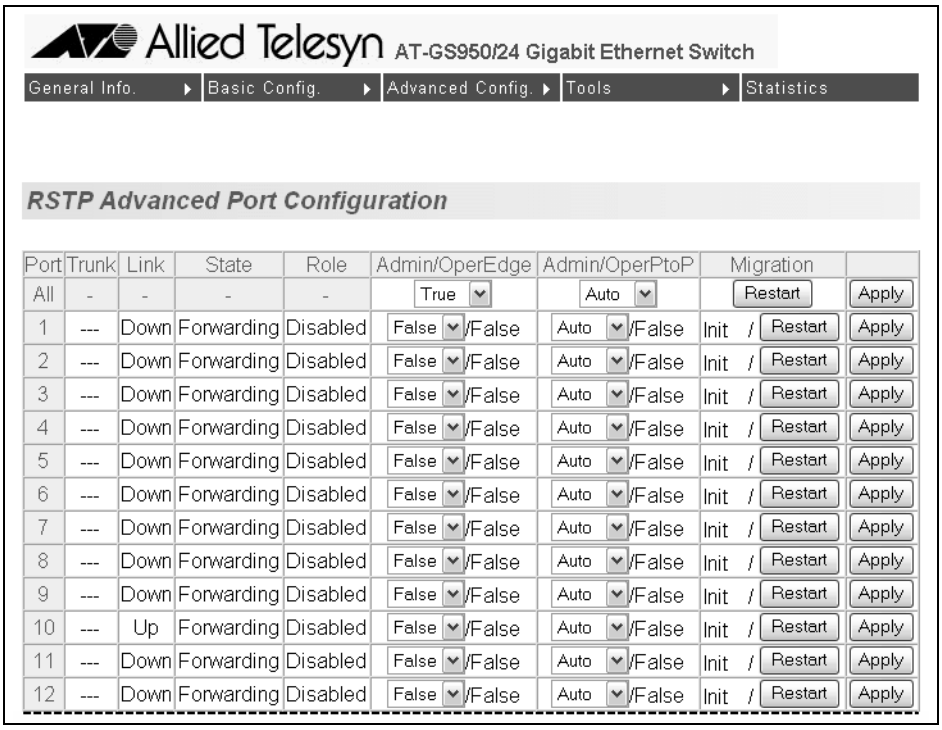


Figure 65. RSTP Advanced Port Configuration Page

2. In the Admin/OperEdge column for the port you want to configure, choose True or False to set whether or not the port will operate as an edge port.

3. In the Admin/OperPtoP column for the port you want to configure, choose a setting based on the information in Table 7.

Table 7. RSTP Point-to-Point Status

Admin	Operation	Port Duplex Operation
Auto	True	Full
	False	Half
True	True	Full or Half
False	False	Full or Half

4. In the Migration column for the port you want to configure, click **Restart** to reset the port.

5. Click **Apply**.

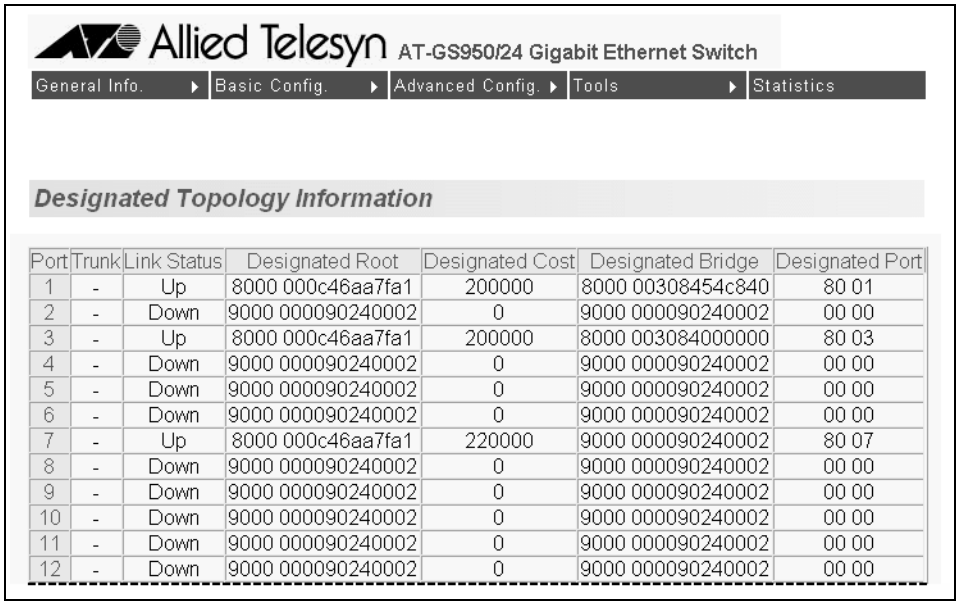
6. To configure all of the ports to the same settings, in the All row, configure one, two, or all of the following settings: Admin/OperEdge, Admin/OperPtoP, and Migration. Click **Apply**.

Viewing the RSTP Topology

To view the current RSTP topology, perform the following procedure:

1. From the Basic Config menu, select **Rapid Spanning Tree** and then **RSTP Topology**.

   The Designated Topology Information page is shown in Figure 66.



Port	Trunk	Link Status	Designated Root	Designated Cost	Designated Bridge	Designated Port
1	-	Up	8000 000c46aa7fa1	200000	8000 00308454c840	80 01
2	-	Down	9000 000090240002	0	9000 000090240002	00 00
3	-	Up	8000 000c46aa7fa1	200000	8000 003084000000	80 03
4	-	Down	9000 000090240002	0	9000 000090240002	00 00
5	-	Down	9000 000090240002	0	9000 000090240002	00 00
6	-	Down	9000 000090240002	0	9000 000090240002	00 00
7	-	Up	8000 000c46aa7fa1	220000	9000 000090240002	80 07
8	-	Down	9000 000090240002	0	9000 000090240002	00 00
9	-	Down	9000 000090240002	0	9000 000090240002	00 00
10	-	Down	9000 000090240002	0	9000 000090240002	00 00
11	-	Down	9000 000090240002	0	9000 000090240002	00 00
12	-	Down	9000 000090240002	0	9000 000090240002	00 00

Figure 66. Designated Topology Information Page

This page displays the following information about the ports:

Trunk
The trunk of which the port is a member.

Link Status
Whether the link on the port is up or down.

Designated Root
The designated root bridge to which the switch's root port is actively connected.

Designated Cost
The sum of all the root port costs on all bridges, including the switch, between the switch and the root bridge.

Designated Bridge
An adjacent bridge to which the root port of the switch is actively connected.

Designated Port
The root bridge to which the root port of the switch is actively connected.

Chapter 22

802.1x Port-based Network Access Control

This chapter contains the procedure for configuring 802.1x port-based network access control:

Note
For background information, refer to “802.1x Port-based Network Access Control Overview” on page 130.

Configuring 802.1x Port-based Network Access Control

To configure 802.1x port-based network access control, perform the following procedure:

1. From the **Advanced Config** menu, select **802.1x**.

   The 802.1x Configuration page is shown in Figure 67.

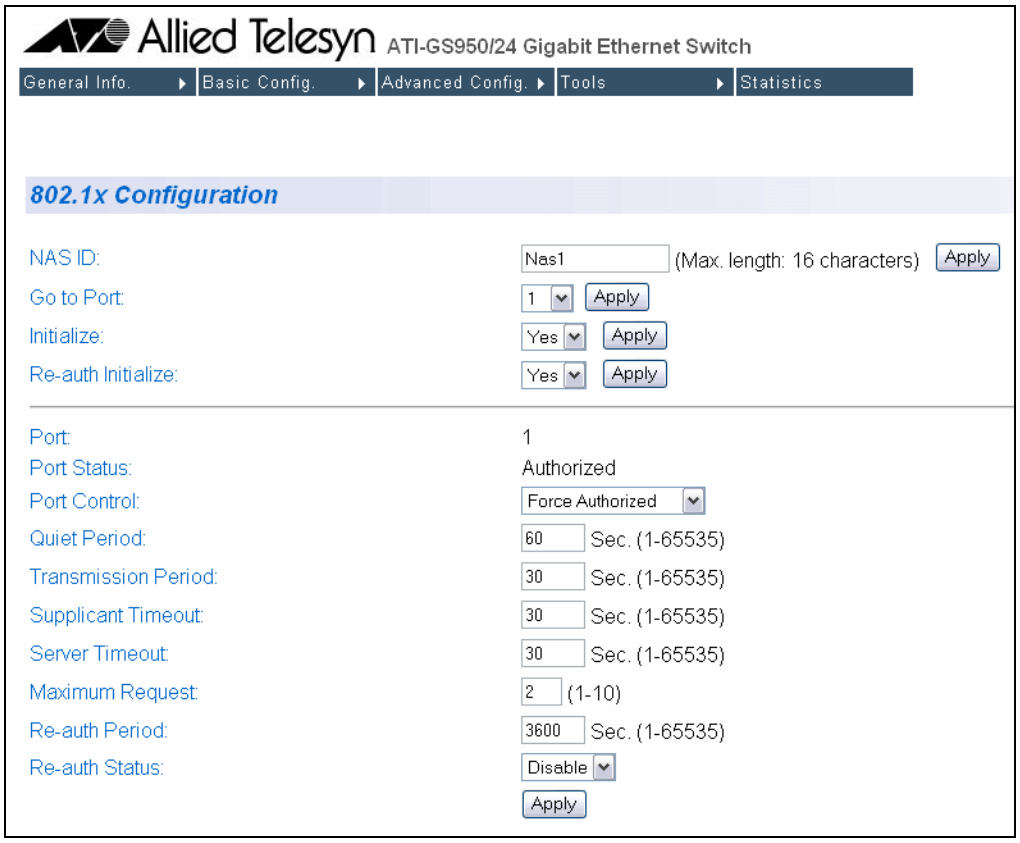


Figure 67. 802.1x Configuration Page

Note
The Initialize and Re-auth Initialize parameters are described in Steps 5 and 6, respectively.

2. To select a port, do the following:

   a. Click **Go To Port** and select the port you want to configure from the pull-down menu. You can configure only one port at a time.

   b. Click **Apply**.

   The current settings for the selected port are displayed.

3. Configure the following parameters as needed. The parameters are defined here:

   NAS ID.
   This parameter assigns an 802.1x identifier to the switch that applies to all ports. The NAS ID can be up to sixteen characters. Valid characters are 0 to 9, a to z, and A to Z. Spaces are allowed. Specifying an NAS ID is optional.

   Port Status.
   Displays the current 802.1 status of the port as either authorized or unauthorized. This is not an adjustable parameter.

   Port Control.
   Sets the 802.1x port control setting. The possible settings are:

   Auto - Enables 802.1x port-based authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes or the port receives an EAPOL-Start packet from a supplicant. The switch requests the identity of the client and begins relaying authentication prompts between the client and the authentication server.

   Force-unauthorized - Places the port in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.

   Force-authorized - Disables IEEE 802.1x port-based authentication and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1x-based authentication of the client. This is the default setting

   Quiet Period.
   Sets the number of seconds that the port remains in the quiet state following a failed authentication exchange with the client. The default value is 60 seconds. The range is 0 to 65,535 seconds.

   Transmission Period.
   Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The default value is 30 seconds. The range is 1 to 65,535 seconds.

   Supplicant Timeout.
   Sets the switch-to-client retransmission time for the EAP-request frame. The default value for this parameter is 30 seconds. The range is 1 to 600 seconds.

   Server Timeout.
   Sets the timer used by the switch to determine authentication server

timeout conditions. The default value for this parameter is 10 seconds. The range is 1 to 60 seconds.

Maximum Request.
Sets the maximum number of times that the switch retransmits an EAP Request packet to the client before it times out the authentication session. The default value for this parameter is 2 retransmissions. The range is 1 to 10 retransmissions.

Re-auth Period.
Specifies the time period between periodic reauthentication of the client. The default value is 3600 seconds. The range is 1 to 65,535 seconds.

Re-auth Status.
Specifies if reauthentication should occur according to the reauthentication period. The options are Enabled or Disabled.

4. When you are finished configuring the parameters, click **Apply** at the bottom of the 802.1x Configuration page.

5. If the port control setting is Auto and you want to return the EAPOL machine state on the port to the initialized state, select **Yes** for the Initialize parameter and click **Apply**.

6. If the port control setting is Auto and you want the node connected to the port to reauthenticate with the RADIUS server, select **Yes** for the Re-auth Initialize parameter and click **Apply**.

Chapter 23

RADIUS Authentication Protocol

This chapter explains how to configure the RADIUS client on the switch. You can use the RADIUS client with 802.1x port-based network access control to control who can forward packets through the switch. The chapter contains the following section:

Note
For background information, refer to “802.1x Port-based Network Access Control Overview” on page 130 and “RADIUS Overview” on page 142.

Configuring the RADIUS Client

To configure the RADIUS client, perform the following procedure:

1. From the **Basic Config** menu, select **RADIUS Config**.

   The RADIUS Server Configuration Menu is shown in Figure 68.

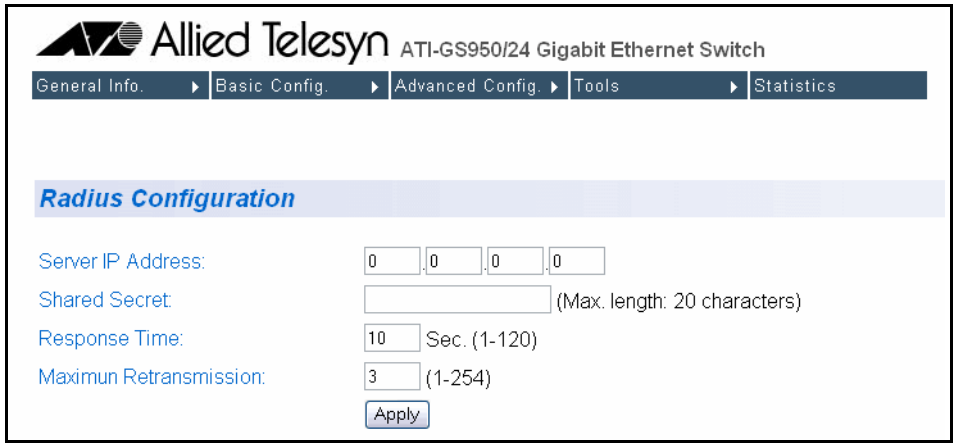


Figure 68. RADIUS Configuration Menu

2. To enter the RADIUS server's IP address, enter the address in the **Server IP Address** field.

3. To specify the server's encryption key, click the **Shared Secret** field and enter the encryption key.

4. To change the response time setting, click the **Response Time** field and enter a new value. The response time is the amount of time in seconds the switch waits for a response from the RADIUS server. The range is 1 to 120 seconds. The default is 10 seconds.

5. To change the maximum retransmissions setting, click the **Maximum Retransmissions** and enter a new value. This parameter specifies the number of times the switch should retransmit to the RADIUS in the event the server does not respond. The range is 1 to 254. The default is 3.

6. Click **Apply** to save your changes.

Chapter 24

Broadcast Storm Control

This chapter contains the procedure for configuring the broadcast storm control feature on the switch. The procedure is:

Note
For background information, refer to “Broadcast Storm Control Overview” on page 148.

Configuring Broadcast Storm Control

To configure the broadcast storm control feature, perform the following procedure:

1. From the **Basic** menu, select **Storm Control**.

   The Broadcast Storm Control page is shown in Figure 69.

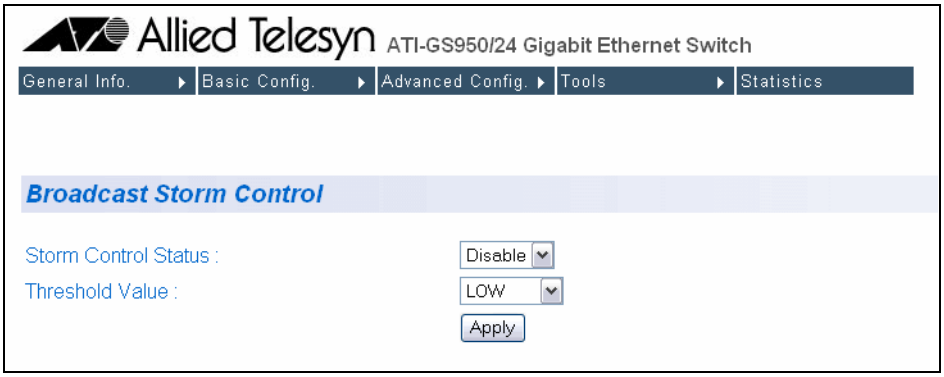


Figure 69. Broadcast Storm Control Page

2. From the Storm Control Status list, select **Enable** to activate the feature or **Disable** to deactivate it. The default setting is disabled.

3. If you are activating the feature, from the Threshold Value list select the desired threshold. Possible values are:

   - High (3000 broadcast packets per second)
   - Medium (500 broadcast packets per second)
   - Low (100 broadcast packets per second)

4. Click **Apply**.

Chapter 25

Management Software Updates

The procedure in this chapter explains how to download a new version of the AT-S79 management software update onto the switch. The procedure is:

- “Downloading a New Management Software Image Using TFTP” on page 234

Note
For information on how to obtain new releases of the AT-S79 management software, refer to “Management Software Updates” on page 14.

Downloading a New Management Software Image Using TFTP

Before downloading a new version of the AT-S79 management software onto the switch, note the following:

- Both models of the AT-GS950 Series use the same AT-S79 software image.
- The current configuration of a switch is retained when a new AT-S79 software image is installed. To return a switch to its default configuration values, refer to “Returning the AT-S79 Management Software to the Factory Default Values” on page 47.
- Your network must have a node with TFTP server software.
- You must store the new AT-S79 image file on the server.
- You should start the TFTP server software before you begin the download procedure.
- The switch where you are downloading the new image file must have an IP address and subnet mask. For instructions on how to configure the IP address on a switch, refer to “Configuring the IP Address, Subnet Mask, and Gateway Address” on page 30 or “Enabling and Disabling the DHCP Client” on page 33.

Caution
Downloading a new version of management software onto the switch causes the device to reset. Some network traffic may be lost during the reset process.

This procedure assumes that you have already obtained the software and have stored it on the computer from which you will be performing this procedure.

To download the AT-S79 image software onto the switch, perform the following procedure:

1. From the **Tools** menu, select **Image Upgrade**.

The Image Upgrade page is shown in Figure 70.

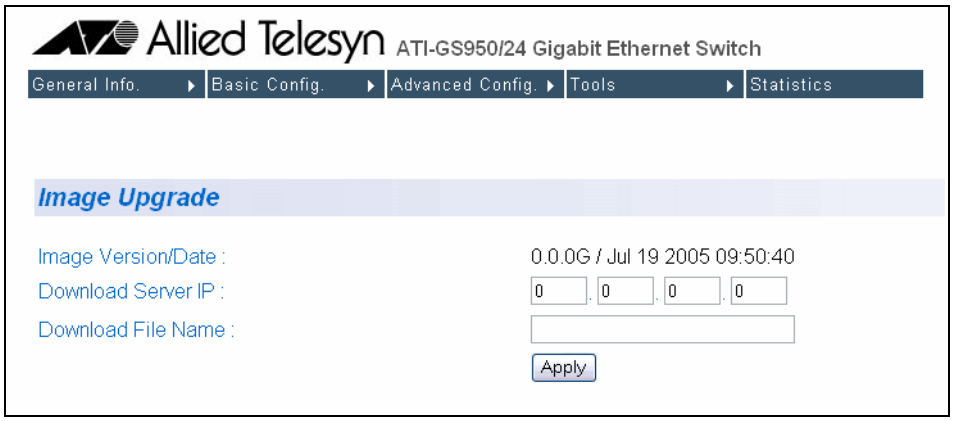


Figure 70. IP Configuration Page

The Image/Version Date shows the current version and date of software installed on the switch.

2. Change the following parameters as necessary:

   Download Server IP
   The IP address of the TFTP server from which you are downloading the new software.

   Download File Name
   The name of the AT-S79 file you are downloading.

3. Click **Apply**.

   The software immediately begins to download onto the switch. This process takes a few minutes. After the software download is complete, the switch initializes the software and reboots. You will lose your web browser connection to the switch during the reboot process.

Appendix A
AT-S79 Software Default Settings

Table 8 lists the factory default settings for the management software.

Table 8. AT-S79 Default Settings

Parameter	Default Setting
IP Configuration	
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway Address	0.0.0.0
DHCP Client	Disabled
System Administration	
System Name	(blank)
System Location	(blank)
System Contact	(blank)
Manager Interface	
Manager Username	manager
Manager Password	manager
Console Idle Timeout	5 minutes
Web Server	Enabled
Ping Configuration	
Target IP Address	0.0.0.0
Number of Requests	10
Timeout	3 seconds
Port Configuration	
Port Status	Enabled
Speed	Auto-Negotiation
Duplex Mode	Auto-Negotiation

Table 8. AT-S79 Default Settings (Continued)

Parameter	Default Setting
Flow Control (Full-duplex Mode)	Enabled
Back pressure (Half-duplex Mode)	Enabled (not adjustable)
Port Mirroring	
Status	Disabled
VLAN	
Name	Default VLAN
VID	1
Ports	All Ports (Untagged)
Quality of Service	
Status	Disabled
Mappings of IEEE 802.1p Priority Levels to Egress Port Priority Queues	See Table 2 on page 97.
Priority Override Status	Disabled
Priority Queue	Queue 0
RSTP	
Status	Disabled
802.1x Port-based Network Access Control	
NAS ID	Nas1
Port Control	Force Authorized
Transmission Period	30 seconds
Supplicant Timeout	30 seconds
Server Timeout	30 seconds
Maximum Requests	2
Quiet Period	60 seconds
Re-authentication Period	3600 seconds
Re-authentication Status	Disabled
RADIUS Client	
Server IP Address	0.0.0.0
Shared Secret	(blank)

Table 8. AT-S79 Default Settings (Continued)

Parameter	Default Setting
Response Time	10 seconds
Maximum Retransmissions	3
Broadcast Storm Control	
Status	Disabled
Threshold	Low
Upgrade Configuration	
TFTP Server IP Address	0.0.0.0
Image Filename	(blank)
Retry Count	5

Index